****

**SYSTEM ZARZĄDZANIA**

**BEZPIECZEŃSTWEM INFORMACJI**

**ROZDZIAŁ I**

**INFORMACJE WSTĘPNE**

System Zarządzania Bezpieczeństwem Informacji opisuje zasady i procedury ochrony informacji przed zagrożeniami w celu zapewnienia ciągłości działania, efektywnego wykorzystania informacji i minimalizacji.

Obejmuje ona ogólne informacje o systemie informatycznym, o zastosowanych rozwiązaniach technicznych, jak również o procedurach eksploatacji i zasadach użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa informacji w Urzędzie Gminy Gorzyce.

Zasady opisane w niniejszym dokumencie są zgodne z obowiązującymi wymaganiami prawnymi, w szczególności:

* § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych
i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Podstawowe definicje:

1. Administrator — oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania informacji w Urzędzie Gminy Gorzyce;
2. Placówka — rozumie się przez to Urząd Gminy Gorzyce;
3. Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji, czyli informacja nie jest ujawniana osobom nieupoważnionym, jest ona dokładna i kompletna oraz dostępna i użyteczna na żądanie upoważnionego personelu;
4. Poufność – zapewnienie dostępu do informacji tylko osobom upoważnionym;
5. Integralność – zapewnienie dostępu do informacji tylko osobom upoważnionym;
6. Dostępność – zapewnienie, że osoby upoważnione będą miały dostęp do informacji tylko wtedy gdy jest to uzasadnione;
7. Przetwarzanie – oznacza operację lub zestaw operacji wykonywanych na informacjach w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
8. Hasło — ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
9. Identyfikator użytkownika — ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania informacji
w systemie informatycznym;
10. Uwierzytelnianie działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
11. Sieć publiczna — publiczna sieć telekomunikacyjna w rozumieniu art. 2 pkt 29 Ustawy z dnia lipca 2004 r. — Prawo telekomunikacyjne;
12. Sieć telekomunikacyjna — sieć telekomunikacyjna w rozumieniu art. 2 pkt 35 Ustawy z dnia lipca 2004 r. — Prawo telekomunikacyjne;
13. System informatyczny — zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania informacji;
14. Teletransmisja — przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.

**ROZDZIAŁ II**

**BEZPIECZEŃSTWO INFORMACJI**

Zarządzanie bezpieczeństwem informacji jest realizowane przez Administratora poprzez zapewnienie warunków umożliwiających wykonanie i egzekwowanie następujących działań:

1. zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2. utrzymywania aktualności inwentaryzacji środków przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3. przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4. podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji, a w razie konieczności bezzwłocznej zmiany tych uprawnień;
5. zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
	1. zagrożenia bezpieczeństwa informacji;
	2. skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna;
	3. stosowanie środków zapewniających bezpieczeństwo informacji, w tym minimalizujących ryzyko błędów ludzkich;
6. zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
	1. monitorowanie dostępu do informacji;
	2. czynności zmierzające do wykrycia nieautoryzowanych działań związanych
	z przetwarzaniem informacji;
	3. zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
7. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
8. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;
9. zawierania w umowach serwisowych podpisanych z wykonawcami zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
10. ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
11. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
	1. dbałości o aktualizację oprogramowania;
	2. minimalizowaniu ryzyka utraty informacji w wyniku awarii;
	3. ochronie przed błędami, utratą, nieuprawnioną modyfikacją;
	4. stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa;
	5. zapewnieniu bezpieczeństwa plików systemowych;
	6. redukcji ryzyka wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;
	7. niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;
	8. kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
12. bezzwłocznego zgłaszania incydentów związanych z bezpieczeństwem informacji
w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
13. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz w roku.

**ROZDZIAŁ III**

**CELE BEZPIECZEŃSTWA INFORMACJI**

1. Celem systemu zarządzania bezpieczeństwem informacji jest zapewnienie poufności,
	1. dostępności i integralności informacji.
2. Zapewnienie poufności oznacza zabezpieczenie informacji przed dostępem nieuprawnionych osób, podmiotów lub procesów.
3. Zapewnienie dostępności oznacza możliwość wykorzystania informacji w dowolnym momencie przez uprawnioną osobę.
4. Zapewnienie integralności oznacza zabezpieczenie informacji przed nieuprawnioną modyfikacją.
5. System zarządzania bezpieczeństwem informacji został zaprojektowany tak, aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią informacje, oraz uzyskać zaufanie zainteresowanych stron.
6. System zarządzania bezpieczeństwem informacji swoim zakresem obejmuje całość funkcjonowania Placówki i wszystkich jej pracowników.
7. Minimalnym wymaganiem dotyczącym zarządzania bezpieczeństwem informacji jest udział w nim wszystkich pracowników Placówki.
8. System zarządzania bezpieczeństwem informacji wdraża się poprzez procedury
i zabezpieczenia wspomagające w zakresie:
	1. nadawania i rejestrowania uprawnień w systemie informatycznym, stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
	2. rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
	3. tworzenia kopii zapasowych, polityki haseł i szyfrowania danych;
	4. sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji i kopii zapasowych;
	5. przekazywania danych poza teren organizacji;
	6. sposobu zabezpieczenia systemu informatycznego przed złośliwym oprogramowaniem;
	7. wykonywania przeglądu i konserwacji systemów oraz nośników informacji;
	8. pracy na urządzeniach mobilnych;
	9. dostępność cyfrową.

**ROZDZIAŁ IV**

**PROCEDURA NADAWANIA I REJESTROWANIA UPRAWNIEŃ**

**W SYSTEMIE INFORMATYCZNYM**

1. Podstawą do nadania uprawnień do systemu informatycznego w Placówce jest upoważnienie dla użytkownika do przetwarzania informacji w systemach teleinformatycznych. Upoważnienie wydawane jest przez Administratora.
2. Zakres uprawnień pracownika nie może być szerszy niż w wydanym upoważnieniu.
3. Za nadawanie uprawnień dostępu do systemów informatycznych oraz za rejestrowanie tych uprawnień odpowiada Administrator.
4. Administrator prowadzi ewidencję osób upoważnionych do dostępu do informacji przetwarzanych w systemach teleinformatycznych.
5. Każdorazowy wniosek o zmianę uprawnienia, ingerujący w poziom dostępu użytkownika do systemów musi być zgłoszony Administratorowi. Procedura przebiega analogicznie jak w przypadku nadania uprawnień dostępu do poziomu systemów.

**ROZDZIAŁ V**

**PROCEDURA ODBIERANIA UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM**

1. Administrator odbiera uprawnienia użytkownika, któremu upłynął termin lub zostało odebrane upoważnienie do przetwarzania informacji, zgodnie z wytycznymi (najczęściej np. w związku z zakończeniem zatrudnienia lub innego stosunku prawnego określającego współpracę z Administratorem, wygaśnięciem lub odwołaniem upoważnienia).
2. Administrator niezwłocznie odbiera uprawnienia użytkownika w systemie informatycznym.
3. Odebranie uprawnień może mieć charakter czasowy lub trwały.
4. Odebranie uprawnień następuje poprzez usunięcie odpowiednich ról z konta użytkownika do czasu ustania przyczyn uzasadniających blokadę (odebranie uprawnień czasowe).
5. Czasowe odebranie uprawnień użytkownika z systemu informatycznego musi nastąpić
w razie:
6. nieobecności użytkownika w pracy trwającej dłużej niż 30 dni kalendarzowych;
7. zawieszenie w pełnieniu obowiązków służbowych.
8. Przyczyną czasowego odebrania uprawnień użytkownika z systemu informatycznego może być:
	1. wypowiedzenie umowy o pracę;
	2. wszczęcia postępowania wobec użytkownika o naruszenie informacji
	(w szczególności wszczęcie postępowania dyscyplinarnego).
9. Przyczyną trwałego odebrania uprawnień z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego użytkownik systemu był zatrudniony.

**ROZDZIAŁ VI**

**STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ**

**PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM**

1. System informatyczny musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło.
2. System informatyczny przetwarzający informacje musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych.
3. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie.
4. Identyfikator jest tworzony automatycznie podczas wprowadzania danych użytkownika do systemu. Hasło do logowania jest tworzone przez użytkownika
w procesie „Przywracania dostępu do konta”.
5. Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:
	* 1. posiadać długość co najmniej 8 znaków;
		2. zawierać litery małe i duże;
		3. zawierać cyfry lub znaki specjalne.
6. Hasło jest zmieniane przez użytkownika nie rzadziej niż co 90 dni lub niezwłocznie
w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby. Hasło powinno różnić się od poprzednio używanych.
7. Użytkownik zobowiązany jest do:
	1. nieujawniania hasta innym osobom, w tym innym użytkownikom;
	2. zachowania hasła w tajemnicy, również po jego wygaśnięciu;
	3. niezapisywania hasła;
	4. postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim;
	5. przestrzegania zasad dotyczących jakości i częstości zmian hasła;
	6. wprowadzenia hasła do systemu w sposób minimalizujący podejrzenie go przez innych użytkowników systemu.
8. W przypadku zapomnienia hasła, użytkownik powinien skorzystać z opcji „Przywróć dostęp do konta” i postępować zgodnie z pojawiającymi się instrukcjami.

**ROZDZIAŁ VII**

**PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UZYTKOWNIKÓW SYSTEMU**

1. Rozpoczynając pracę w systemie informatycznym użytkownik:
2. włącza listwę podtrzymującą napięcie, włącza zasilanie awaryjne (UPS) i uruchamia komputer;
3. wprowadza niezbędne do pracy identyfikatory i hasła;
4. hasła są wprowadzane w sposób minimalizujący ryzyko podejrzenia ich przez osoby trzecie;
5. w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, natychmiast kontaktuje się z Administratorem;
6. w przypadku niestandardowego zachowania aplikacji przetwarzającej informacje pracownik natychmiast powiadamia o zaistniałym fakcie Administratora.
7. Zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy), użytkownik blokuje stację roboczą. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej po wprowadzeniu hasła, w sposób gwarantujący jego niepodejrzenie przez osoby trzecie.
8. Opuszczając pomieszczenie, w którym przetwarzane są informacje, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona do przebywania w tym pomieszczeniu. Zabronione jest pozostawienie bez nadzoru w pomieszczeniach osób nieupoważnionych.
9. Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzić wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.
10. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do informacji powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.
11. Kończąc pracę w systemie informatycznym, pracownik wylosowuje się ze wszystkich aplikacji, z których korzystał, wyłącza stację roboczą i zabezpiecza nośniki danych.
12. Zabrania się wyłączać komputery w czasie działania programu przyciskiem „POWER”, gdyż takie działanie może spowodować trwałe uszkodzenie zbiorów danych. Nie należy wyłączać przewodów zasilających i sieciowych z gniazda elektrycznego;
13. Użytkownik powinien zaczekać przy komputerze do chwili jego wyłączenia.
14. W przypadku gdy pracownik jest ostatnią osobą opuszczającą pomieszczenie, sprawdza zamknięcie okien, zamyka na klucz drzwi do pomieszczenia oraz zdaje klucze
w sekretariacie.

# **ROZDZIAŁ VIII**

**PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH, POLITYKI HASEŁ I SZYFROWANIA DANYCH**

1. Kopie bezpieczeństwa nie mogą być wykonywane rzadziej niż raz na tydzień. Nie zaleca się dokonywania kompresji bazy danych.
2. Administrator odpowiada za zabezpieczenie wykonywania kopii zapasowych.
3. Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika,
w sposób uniemożliwiający odczytanie zapisanych na nich danych.

**ROZDZIAŁ IX**

**SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH**

**NOŚNIKÓW INFORMACJI I KOPII ZAPASOWYCH**

1. Nośniki danych zarówno w postaci elektronicznej jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją
i zniszczeniem. Informacje mogą być zapisywane na nośnikach przenośnych
w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
2. Informacje przechowywane są na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane. Po ustaniu czasu przechowywania zawartości nośnika podlega skasowaniu przy użyciu narzędzi zaakceptowanych do użycia w Placówce,
a w przypadku nośników optycznych stosuje się niszczenie w niszczarkach umożliwiających niszczenie tego typu nośników.
3. Nośniki informacji oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do tego i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników informacji i wydruków poza budynek Placówki powinno odbywać się za zgodą Administratora.
4. W przypadku, gdy nośnik informacji nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie informacji. Jeżeli wydruk nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.
5. Na terenie Placówki zabrania się kopiowania informacji z nośników magnetycznych
i optycznych, także w formie papierowej, zawierające informacje dotyczące działalności Placówki — bez zgody Administratora.
6. Zabrania się wnoszenia i używania jakichkolwiek prywatnych lub innych „niesłużbowych” nośników magnetycznych, optycznych oraz pamięci przenośnych bez zgody Administratora.
7. W przypadku wycofania sprzętu komputerowego z użycia informacje na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych zaakceptowanego do użycia w Placówce. W przypadku braku możliwości programowego usunięcia danych dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada użytkownik po uzyskaniu zgody od Administratora na ich zniszczenie. Zniszczenie nośnika jest potwierdzone protokołem przechowywanym przez Administratora.

**ROZDZIAŁ X**

**PRZEKAZYWANIE DANYCH POZA TEREN ORGANIZACJI**

1. Dane przekazywane poza teren Placówki, za pomocą łączy internetowych lub na nośnikach elektronicznych, muszą być odpowiednio zabezpieczone (w szczególności szyfrowane).
2. Przekazywane informacje muszą być zabezpieczone w taki sposób by ich nieuprawnione odczytanie było niemożliwe.
3. Haseł dostępu, czy kluczy aktywacyjnych do danych nie można przekazywać tą samą drogą, co danych.
4. Dane na nośnikach muszą być zabezpieczone programem szyfrującym.

**ROZDZIAŁ XI**

**SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED ZŁOŚLIWYM OPROGRAMOWANIEM**

1. System informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu.
2. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:
	1. uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w Placówce;
	2. samowolnego korzystania z nośników przenośnych;
	3. otwierania poczty elektronicznej, której tytuł nie sugeruje związku
	z pełnionymi obowiązkami służbowymi;
	4. korzystania z Internetu w celach niezwiązanych z pełnionymi obowiązkami służbowymi;
	5. podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów.
3. W celu zapewnienia ochrony antywirusowej, na wszystkich komputerach będących
w posiadaniu Placówki, został zainstalowany program antywirusowy, który jest na bieżąco aktualizowany. Na styku sieci wewnętrznej z siecią publiczną został zlokalizowany firewall.
4. Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:
5. załączniki do poczty elektronicznej,
6. przeglądane strony internetowe,
7. pliki i aplikacje pochodzące z nośników wymiennych uruchamiane
i odczytywane na stacji roboczej.
8. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić Administratora. Do objawów powyższych można zaliczyć:
	1. istotne spowolnienie działania systemu informatycznego,
	2. nietypowe działanie aplikacji,
	3. nietypowe komunikaty,
	4. utratę danych lub modyfikację danych.
9. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:
	1. oprogramowanie antywirusowe,
	2. zaporę sieciową,
	3. aktualizację oprogramowania systemowego,
10. Administrator jest odpowiedzialni za nadzór nad działaniem zabezpieczeń.

**ROZDZIAŁ XII**

**PROCEDURY WYKONYWANIA PRZEGLĄDU I KONSERWACJI SYSTEMÓW**

**ORAZ NOŚNIKÓW INFORMACJI**

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2. Przegląd i konserwacja sprzętu informatycznego realizowana jest przez pracowników Placówki wyznaczonych przez Administratora lub przez upoważnionych przedstawicieli podmiotów zewnętrznych.
3. Prace serwisowe wykonywane na terenie Palcówki przez podmioty zewnętrzne, podlegają bezpośredniemu nadzorowi przez pracownika Placówki wyznaczonego przez Administratora.
4. Przekazanie sprzętu teleinformatycznego do naprawy poza teren Placówki jest dopuszczalne, jeżeli spełnione zostały poniższe warunki:
	1. sprzęt przekazywany jest bez nośników zawierających informacje;
	2. przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.

**ROZDZIAŁ XIII**

**KORZYSTANIE Z INTERNETU**

1. Użytkownikom zabrania się dostępu do Internetu za pośrednictwem łączy, które nie są autoryzowane przez osoby upoważnione. Osobą upoważnioną jest w tym wypadku Administrator.
2. Zabrania się korzystania z Internetu w sposób mogący narazić Administratora na jakiekolwiek straty finansowe lub inną szkodę majątkową i niemajątkową.
3. Pracownicy, którzy posiadają dostęp do łączy internetowych, zobowiązani są do ich wykorzystywania wyłącznie w celach służbowych z jednoczesnym zachowaniem dobrych obyczajów i poszanowania praw autorskich i ich dzieł udostępnianych przez sieć Internet.
4. Niedozwolone dla pracownika jest:
	1. udostępnianie osobom trzecim nazw kont i haseł;
	2. samodzielna zmiana konfiguracji stacji roboczych związanych ściśle
	z przyłączem internetowym;
	3. ściąganie i instalowanie oprogramowania z Internetu bez zgody Administratora nawet w przypadkach, gdy ww. oprogramowanie jest darmowe.
5. Nie przestrzeganie zasad określonych w ust. 4 będzie traktowane jak naruszenie obowiązków pracowniczych. O zaistniałym fakcie przełożony pracownika powiadamia Administratora.
6. Uzyskiwanie dostępu, przeglądanie lub rozprowadzanie niewłaściwych materiałów
(np. rozrywkowych, pornografii) poprzez sieć wewnętrzną Administratora lub sieć Internet jest surowo zabronione.
7. Niedopuszczalne jest ujawnianie za pośrednictwem Internetu informacji prawnie chronionych.
8. Korzystanie z czasu wyznaczonego na wykonywanie obowiązków służbowych
i zasobów Placówki w celu osiągnięcia osobistych korzyści jest zakazane.

**ROZDZIAŁ XIV**

**PRACA NA URZĄDZENIACH MOBILNYCH**

1. Użytkownik, któremu zostało powierzone urządzenie mobilne, powinien chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas transportu takiego urządzenia.
2. Obowiązuje zakaz używania urządzenia mobilnego przez osoby inne niż użytkownicy, którym zostały one powierzone.
3. Przy pracy na urządzeniach mobilnych powinno zwrócić się szczególną uwagę na podłączanie ich do nieznanych sieci bezprzewodowych.
4. Każdy użytkownik urządzenia mobilnego powinien je zabezpieczyć przed możliwością włączenia przez osoby nieuprawnione.
5. Pliki zawierające informacje i przechowywane na urządzeniach mobilnych powinny być zaszyfrowane i obowiązkowo zabezpieczone hasłem. Szyfrowane mogą być same pliki lub pliki mogą się znajdować na zaszyfrowanej części urządzenia.

**ROZDZIAŁ XV**

**STRONA INTERNETOWA, SKRZYNKA ePUAP, BIULETYN INFORMACJI PUBLICZNEJ**

1. Placówka prowadzi stronę Biuletynu Informacji Publicznej.
2. Placówka posiada Elektroniczną skrzynkę podawczą - ePUAP, której adres jest dostępny na jej stronie internetowej oraz na Biuletynie Informacji Publicznej.
3. Placówka zapewnia dostępność cyfrową na poziomie Web Content Accessibility Guidelines (WCAG 2.1):
	1. strony podmiotowej Biuletynu Informacji Publicznej;
	2. następujących elementów funkcji strony internetowej:
		1. danych teleadresowych podmiotu publicznego oraz linku do strony podmiotowej Biuletynu Informacji Publicznej podmiotu publicznego, jeżeli na podstawie odrębnych przepisów podmiot publiczny jest obowiązany do jej prowadzenia,
		2. narzędzi służących do kontaktu z podmiotem publicznym,
		3. nawigacji,
		4. deklaracji dostępności strony internetowej lub aplikacji mobilnej podmiotu publicznego, zwanej dalej „deklaracją dostępności”,
		5. informacji dotyczących sytuacji kryzysowej w rozumieniu art. 3 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2018 r. poz. 1401 i 1560) oraz innych informacji związanych z bezpieczeństwem publicznym, publikowanych przez podmiot publiczny,
		6. dokumentów urzędowych oraz wzorów umów lub wzorów innych dokumentów przeznaczonych do zaciągania zobowiązań cywilnoprawnych.
4. Placówka sporządza i umieszcza deklarację dostępności w sposób dostępny cyfrowo na stronie internetowej oraz na Biuletynie Informacji Publicznej.

**ROZDZIAŁ XVI**

**ODPOWIEDZIALNOŚĆ UŻYTKOWNIKA**

1. Zasady i procedury zawarte w niniejszej Instrukcji obowiązują wszystkie osoby wykonujące zadania w Placówce Administratora bez względu na stosunek prawny stanowiący podstawę współpracy.
2. Instalacje oprogramowania na stanowiskach pracowniczych mogą dokonywane być
z nośników znajdujących się w zasobach Administratora. Ich instalacja może być dokonywana przez pracownika Placówki wyznaczonego przez Administratora.
3. Każdy pracownik jest indywidualnie odpowiedzialny za powierzony mu sprzęt. Użytkownicy nie mogą sami dokonywać jakiejkolwiek zmiany komponentów sprzętu komputerowego, ani przyłączać własnych komponentów.
4. Wszelkie zapotrzebowanie na dodatkowe komponenty takie jak: RAM, dysk twardy, karta sieciowa, napęd optyczny i inne muszą być zgłaszane za pośrednictwem Administratora do pracownika Placówki wyznaczonego przez Administratora, który osobiście dokonuje zmian.
5. Sprzęt komputerowy nie może być wynoszony poza teren Placówki lub przenoszony
w inne miejsce bez wcześniejszej zgody Administratora.
6. Utrata lub kradzież sprzętu powinna być niezwłocznie zgłaszana Administratorowi.
7. Każdy pracownik jest indywidualnie odpowiedzialny za przechowywane przez siebie informacje w formie tradycyjnej (papierowej) jak i w formie elektronicznej.
8. Za umożliwienie korzystania z komputera przez osobę nieupoważnioną odpowiada użytkownik, któremu sprzęt ten został przydzielony.
9. Na każdym użytkowniku systemu informatycznego spoczywa odpowiedzialność za przetwarzanie informacji w ramach przydzielonych mu uprawnień systemowych
i programowych, oraz odpowiedzialność za ochronę ich przed niepowołanym dostępem, niepowołaną modyfikacją, zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu informacji.

**ROZDZIAŁ XVII**

**AUDYT WEWNĘTRZNY**

Przynajmniej raz w roku w danej placówce powinien zostać przeprowadzony audyt bezpieczeństwa informacji.

Administrator wyznacza pracownika lub zleca go osobom/podmiotom z zewnątrz do przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji, tak, aby uzyskać zapewnienie o ich ciągłej przydatności, adekwatności i skuteczności.

Osoby odpowiedzialne za przeprowadzanie audytów obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny posiadać odpowiednie kwalifikacje.