Załącznik do Zarządzenia Nr 91/2024
Starosty Wąbrzeskiego
z dnia 12 grudnia 2024 roku

# POLITYKA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM w STAROSTWIE POWIATOWYM w WĄBRZEŹNIE

UWAGA:
Dokument wyłącznie
do użytku wewnętrznego

**Zatwierdzam:**

……...
data i podpis Administratora

## § 1
## Postanowienia Ogólne

1. Polityka określa zasady oraz tryb postępowania przy przetwarzaniu informacji w systemach informatycznych w celu zapewnienie bezpieczeństwa tych informacji zgodnie z Rozporządzenia Parlamentu Europejskiego i Rady(UE) Nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – EODO) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247).
2. Przez zapewnienie bezpieczeństwa informacji należy rozumieć zachowanie:
    1) **poufności** - daje gwarancję, że informacje są dostępne tylko i wyłącznie dla autoryzowanych osób - pracowników, posiadających prawo dostępu do tych informacji,
    2) **integralności** - zabezpiecza ona dokładność i kompletność zarówno informacji, jak też i stosowanych metod jej ochrony oraz zapewnia, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
    3) **dostępności** - gwarancja, że użytkownicy posiadający stosowne uprawnienia mają stały dostęp do informacji i zgromadzonych zasobów,
    4) **rozliczalności** - zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko jemu,
    5) **autentyczności** - zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
    6) **niezaprzeczalności** – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
    7) **niezawodności** – zapewnienie spójności oraz zamierzonych zachowań i skutków, co można interpretować jako poprawność danych i właściwą ich interpretację.
3. Przestrzeganie zasad i procedur zawartych w instrukcji ma na celu zmniejszenie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Systemie Informatycznym w zakresie zidentyfikowanych zagrożeń:
    1) włamania do systemu informatycznego i pozyskania informacji przez osoby nieuprawnione.
    2) pozyskania informacji przez osoby nieuprawnione na skutek bezpośredniego dostępu do komputera,
    3) pozyskania informacji przez osoby nieuprawnione w trakcie przesyłania ich siecią publiczną (INTERNET),
    4) dokonywania modyfikacji informacji przez osoby nieuprawnione,
    5) utraty informacji bądź jej dezintegracji,
    6) utraty czasowej dostępności do informacji.
4. Podstawowe pojęcia:
    1) **Administrator –** Starostwo Powiatowe w Wąbrzeźnie w imieniu, którego działa Starosta Wąbrzeski.
    2) **Inspektor Ochrony Danych** – osoba wyznaczona przez administratora lub podmiot przetwarzający na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, zwany dalej inspektorem.

3) **Administrator sytemu informatycznego (ASI) - Informatyk** – osoba wyznaczona przez administratora odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych do przetwarzania informacji i danych osobowych, zwany dalej informatykiem lub ASI. W przypadku niewyznaczenia informatyka, jego obowiązki pełni administrator.
4) **System do przetwarzania informacji w tym danych osobowych** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych, zwany dalej system TI.
5) **Identyfikator** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych
w systemie informatycznym
6) **Hasło –** rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi.
7) **Użytkownik systemu** - osoba upoważniona przez administratora lub podmiot przetwarzający do przetwarzania informacji i danych osobowych, której przyznano uprawnienia do przetwarzania danych osobowych w systemie do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu, zwany dalej użytkownikiem.

5. Wzory dokumentów określone w załącznikach do polityki mogą być zastąpione innymi wzorami dokumentów jednakże zgodnymi z zasadami określonymi niniejszej polityce.

**§ 2**
**System teleinformatyczny**

1. Przetwarzanie danych osobowych odbywa się na:
   1) serwerze,
   2) stacjach roboczych użytkowników,
   3) urządzeniach mobilnych takich m.in. jak laptopy, smartfony, tablety itp.
   4) urządzeniach peryferyjnych takich m.in. jak: drukarki, skanery, faxy itp., a także w sposób zdalny i mobilny.
2. Sprzęt informatyczny połączony jest z siecią publiczną z wyjątkiem rejestrów państwowych, które przekazano do przetwarzania administratorowi.
3. Przetwarzanie danych odbywa się także w sposób zdalny i mobilny.
4. Informacje dotyczące sprzętu informatycznego oraz oprogramowania stosowanego do przetwarzania danych osobowych zawiera zał. nr 1.

**§ 3**
**Poziom bezpieczeństwa**

1. Uwzględniając kategorie danych osobowych i informacji przetwarzanych przez administratora oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie TI połączonym z siecią publiczną, wprowadza się wysoki poziom bezpieczeństwa, który zostanie uzyskany przy zastosowaniu n/wym. zasad.
2. Zabezpieczenie obszaru przetwarzania danych w tym infrastruktury informatycznej i telekomunikacyjnej realizowane jest przez:
   1) zabezpieczenie obszaru przetwarzania danych przed dostępem osób nieuprawnionych podczas nieobecności upoważnionych pracowników administratora;
   2) nadzór osób upoważnionych nad przebywającymi w obszarze przetwarzania danych osobami nieuprawnionymi;
   3) kontrolę dostępu do pomieszczeń serwerowni.
   4) zabezpieczenia przed skutkami awarii zasilania (UPS) dla serwerów i pozostałych kluczowych elementów systemu,
   5) autonomiczne klimatyzatory w pomieszczeniach serwerowni.

3. Urządzenia i nośniki zawierające dane przekazywane poza obszar przetwarzania danych, zabezpiecza się w sposób zapewniający ich poufność i integralność.
4. Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii transmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz.
5. Wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej stosuje się środki kryptograficznej ochrony.
6. Przesyłanie poczty elektronicznej odbywa się za pomocą łącza szyfrowanego odpowiadającego właściwościom certyfikatu SSL.
7. Przeglądarki internetowe stanowisk komputerowych domyślnie ustawione są w sposób uniemożliwiający automatyczne uzupełnianie formularzy i haseł dostępu do kont pocztowych i programów.
8. Zasady korzystania z sieci bezprzewodowej - wifi:
    1) W siedzibie administratora funkcjonuje ogólnodostępna sieć bezprzewodowa (HOTSPOT), zapewniająca połączenie z siecią Internet
    2) Sieć jest odseparowana dla klientów, bez dostępu do sieci LAN.
    3) Korzystanie z tej sieci jest ograniczone przez administratora poprzez blokadę stron z treściami nieodpowiednimi dla powagi urzędu – uznawanymi za nieetyczne lub obraźliwe
    4) Sieć WiFi administratora zabezpieczona jest poprzez zastosowanie protokołu WPA2 na poziomie stanowisko – sieć, dostęp do sieci jest opatrzony hasłem,
    5) hasło posiada minimum 8 znaków zawierających duże i małe litery cyfrę oraz znak specjalny,
    6) hasło nie podlega zmianie.
9. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:
    1) zastosowanie środków ochrony przed szkodliwym oprogramowaniem,
    2) użycie systemu Firewall do ochrony dostępu do sieci komputerowej,
    3) aktualizację oprogramowania systemowego, a w razie zakończenia wsparcia przez producenta oprogramowania, wybór i zainstalowanie innego spełniającego wymogi aktualnego bezpieczeństwa,
    4) zainstalowanie na komputerach programów antywirusowych,
    5) centralnie zarządzany system antywirusowy pozwalający monitorować stan oprogramowania antywirusowego na stanowiskach komputerowych,
    6) regularne skanowanie stanowisk komputerowych programem antywirusowym zgodnie z harmonogramem
    7) skanowanie stanowisk komputerowych programem antywirusowym wg potrzeb i zaleceń informatyka,
    8) zainstalowanie na serwerach i stanowiskach komputerowych użytkowników wyłącznie programów spełniających wymogi legalności,
    9) mechanizm wymuszający skanowanie zewnętrznych nośników informacji na obecność wirusów i innego szkodliwego oprogramowania przed ich użyciem na stanowisku komputerowym,
10. System Informatyczny jest chroniony przed zagrożeniami pochodzącymi z sieci publicznej przez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem poprzez:
    1) monitorowanie stanowisk komputerowych użytkowników pod kątem legalności oprogramowania,
    2) zablokowanie dostępu do kategorii stron internetowych, które mogą wpływać na obniżenie poziomu bezpieczeństwa przetwarzania danych systemu,
    3) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa,
    4) mechanizmy monitorujące aktywność użytkowników w sieci publicznej,
    5) mechanizm wymuszający okresową zmianę haseł dostępu,
    6) przydzielanie uprawnionym indywidualnych identyfikatorów,
    7) mechanizm uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

8) zakaz ponownego stosowania identyfikatorów, które utracił ważność,
9) mechanizmy pozwalające na określenie odpowiednich praw dostępu do danych dla poszczególnych użytkowników, informatyka i administratora,
10) mechanizm automatycznego wygaszania ekranów na stanowiskach komputerowych po upływie 5 min. bezczynności i konieczność ponownego zalogowania do systemu po wznowieniu pracy,
11) mechanizm wymuszający ponowne zalogowanie do systemu po wznowieniu pracy na stanowisku komputerowym.

11. Zabezpieczenie systemu do przetwarzania danych przed zagrożeniami pochodzącymi z sieci publicznej realizowane jest przez:
    1) odseparowanie sieci obsługującej przetwarzanie rejestrów państwowych,
    2) blokowanie nieuprawnionego dostępu do sieci administratora z sieci publicznej,
    3) ustalenie reguł zdalnego serwisu użytkowanych programów,
    4) ograniczenie kategorii dostępnych stron WWW,
    5) kontrolę antywirusową odwiedzanych stron WWW,
    6) kontrolę antywirusową treści informacji przekazywanych do i z sieci publicznej,
    7) ewidencję wszystkich połączeń z siecią publiczną,
    8) kontrolę antywirusową treści informacji przekazywanych do i z sieci publicznej,
    9) generowanie okresowych raportów o wykorzystaniu dostępu do sieci publicznej.

## § 4
## Zasady korzystania z sieci Internet

1. Strony WWW mogące być źródłem ataków lub szkodliwego oprogramowania są niedostępne dla użytkowników.
2. Wykaz kategorii i adresów stron internetowych zablokowanych w systemie informatycznym stanowi zał. nr 2.
3. O zablokowaniu dostępu do strony WWW niezbędnej do wykonywania czynności służbowych, użytkownik informuje informatyka, podając pełny adres zablokowanej strony; jeżeli dostęp został zablokowany przypadkowo, to po pozytywnej weryfikacji zawartości strony WWW informatyk odblokowuje ją, a w przypadkach wątpliwych, o odblokowaniu strony WWW decyduje administrator.
4. Informatyk może odmówić odblokowania strony WWW, jeżeli w wyniku tego obniżyłby się poziom bezpieczeństwa sytemu i sieci.
5. Zdalny dostęp do systemu z sieci publicznej, a w szczególności do aplikacji służących do przetwarzania danych osobowych jest możliwy jedynie przy zastosowaniu technicznych zabezpieczeń zapewniających rozliczalność, autentyczność i niezaprzeczalność osób, a także integralność i poufność przetwarzanych danych. Dostęp realizowany jest przy wykorzystaniu szyfrowanych protokołów transmisji danych.
6. Dostęp do systemu z sieci publicznej jest możliwy dla osób i podmiotów do tego uprawnionych i dotyczy to następujących sytuacji:
    1) świadczenia serwisu zdalnego:
        a) dostęp w ramach zawartych umów dotyczących serwisu oprogramowania zainstalowanego w systemie - na czas trwania umowy, zasady dostępu do danych osobowych precyzuje zawarta dodatkowo umowa powierzenia przetwarzania danych osobowych pomiędzy administratorem, a podmiotem, który świadczy usługi serwisowe,
        b) dostęp jest możliwy wyłącznie na czas wykonywania prac serwisowych i jest blokowany po ich zakończeniu,
        c) dostęp polegający na zdalnej kontroli pulpitu użytkownika jest możliwy tylko za pomocą licencjonowanych narzędzi programowych zapewniających szyfrowanie transmisji;
    2) wykonywania czynności kontrolnych, konserwacyjnych, diagnostycznych oraz naprawczych przez informatyka.

7. Informatyk może ograniczyć lub zablokować dostęp do sieci publicznej użytkownikowi nie przestrzegającemu zasad polityki ochrony danych.
8. Informatyk może ograniczyć lub zablokować dostęp do sieci publicznej użytkownikowi nie przestrzegającemu zasad niniejszej polityki.

**§ 5**

**Procedura nadawania, zmiany, zawieszenia i cofnięcia uprawnień do przetwarzania danych w systemie TI oraz stosowane środki uwierzytelnienia.**

1. Uprawnienia do systemu informatycznego otrzymuje wyłącznie osoba posiadająca upoważnienie administratora wydane zgodnie z politykami bezpieczeństwa informacji stosowanymi przez administratora.
2. Tworzy się dwa konta administratora służące do zarzadzania systemem serwera. Oba konta posiadają te same uprawnienia w zakresie zarządzania systemem z wyjątkiem wzajemnej możliwości haseł dostępowych.
    1) Pierwsze konto o identyfikatorze - ASI - zarządzane jest przez informatyka.
    2) Drugie konto o identyfikatorze – admin – tworzone jest dla administratora. Hasło do konta nadawane jest przy pierwszym uruchomieniu serwera.
3. Hasła do kont składają się min. z 8 znaków zawierających cyfry, duże i małe litery oraz znak specjalny.
4. Hasło do konta – ASI – zmieniane jest raz na rok, hasło to nie może być podobne do12 ostatnio używanych.
5. Hasło do konta admin przechowywane jest w zapieczętowanej kopercie przez- administratora. Hasło to podlega użyciu w przypadku wystąpienia naruszenia bezpieczeństwa systemu informatycznego do przetwarzania danych lub braku możliwości wykorzystania konta – ASI
6. Wykorzystanie hasła do konta – admin 2 podlega pisemnemu udokumentowaniu.
7. Uprawnienia oraz zmiany w zakresie uprawnień do kont ASI i admin określa administrator zgodnie ze wzorem - zał. nr 3 do polityki.
8. W procesie uwierzytelnienia użytkowników systemu TI wykorzystywane są identyfikatory i hasła.
9. Nadawanie, cofnięcie, zmianę lub zawieszenie uprawnień do systemu TI lub poczty elektronicznej następuje na podstawie wniosku przełożonego pracownika, a w przypadku osoby nie będącej pracownikiem na wniosek przełożonego pracownika koordynującego lub nadzorującego pracę takiej osoby zgodnie ze wzorem - zał. nr 3 do polityki.
10. Wnioski o nadanie, zmianę, zawieszenie i cofnięcie uprawnień przechowuje informatyk.
11. Uprawnienia do systemu TI na podstawie wniosku przydziela informatyk.
12. W przypadku nadawania użytkownikowi systemu uprawnień do danego systemu informatycznego po raz pierwszy, informatyk dokonuje nadania użytkownikowi systemu identyfikatora oraz adresu poczty elektronicznej i wygenerowania hasła.
13. Identyfikator użytkownika w systemie informatycznym oraz adres poczty elektronicznej musi być unikalny dla użytkownika i zawierać minimum 3 znaki.
14. Zabronione jest stosowanie identyfikatora, który w przeszłości był już stosowany w systemie TI. Sprawdzenie unikalności identyfikatora dokonuje informatyk na podstawie wniosków o nadanie uprawnień do przetwarzania informacji i danych osobowych.
15. Odbiór identyfikatora do systemu i adres poczty elektronicznej oraz hasło pierwszego logowania użytkownik systemu TI kwituje we wniosku – wzór zał. nr 3.
16. Zasady określające proces uwierzytelniania obowiązują w przypadku pracy na stacjonarnym, jak i mobilnym sprzęcie informatycznym.
17. Hasła dostępu do systemu informatycznego z wyjątkiem urządzeń mobilnych typu smartfon, tablet, terminal mobilny muszą spełniać poniższe warunki:
    1) posiadać długość co najmniej 8 znaków,
    2) zawierać litery małe i duże,
    3) zawierać cyfry i znaki specjalne.
18. Użytkownik systemu jest zobowiązany do zmiany hasła nie rzadziej niż co 1 miesiąc,

chyba że zmiana hasła jest wymuszona przez system informatyczny lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby. Jeżeli użytkownik nie posiada uprawnień do zamiany hasła, czynność tą wykonuje informatyk.

19. Hasło powinno różnić się od poprzednio stosowanego lub 12 poprzednio stosowanych.
20. Informatyk przekazując dane pierwszego logowania przeprowadza szkolenie użytkownika systemu wskazując zasady korzystania ze sprzętu informatycznego oraz poczty elektronicznej.
21. Użytkownik po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet jeżeli system informatyczny nie wymusza takiego działania.
22. Na stanowiskach komputerowych, dopuszcza się zastosowanie konta z uprawnieniami „gość" nieopatrzonego hasłem.
23. Użytkownik systemu zobowiązany jest do:
    1) nieujawniania hasła innym osobom, w tym innym użytkownikom,
    2) zachowania hasła w tajemnicy, również po jego wygaśnięciu,
    3) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim,
    4) przestrzegania zasad dotyczących jakości i częstości zmian hasła,
    5) wprowadzania hasła do systemu w sposób minimalizujący ujawnianie go przez innych użytkowników systemu.
24. Wykorzystanie identyfikatora i hasła innego użytkownika, w tym w ramach pełnionego zastępstwa, stanowi naruszenia zasad bezpieczeństwa informacji i może naruszać podstawowe obowiązki pracownicze.
25. Monitor stanowiska komputerowego powinien być ustawiony w taki sposób, aby uniemożliwić wgląd w dane przebywającym w pomieszczeniu osobom nieupoważnionym.
26. W przypadku zapomnienia hasła użytkownik systemu powinien zwrócić się do informatyka o wygenerowanie nowego hasła.
27. W przypadku stwierdzenia naruszenia bezpieczeństwa informacji w związku z utratą poufności hasła użytkownik systemu jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie informatyka oraz bezpośredniego przełożonego, który podejmuje działania zgodnie z § 12 niniejszej polityki. W innym przypadku informatyk nadaje użytkownikowi nowe hasło logowania i pisemnie dokumentuje tą czynność.

## § 6
## Procedura rozpoczęcia, zawieszenia i zakończenia pracy w systemie TI

1. Rozpoczynając pracę w systemie informatycznym użytkownik systemu:
    1) uruchamia komputer,
    2) wprowadza identyfikatory i hasła,
    3) w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, weryfikuje poprawność wpisanych znaków (capslook, num lock, układ klawiatury), jeśli te czynności okażą się nieskuteczne kontaktuje się z informatykiem.
2. Zawieszenie pracy na stanowisku komputerowym:
    1) użytkownik, opuszczający czasowo stanowisko pracy, wyloguje się, przez użycie kombinacji klawiszy Windows+L,
    2) w przypadku, gdy użytkownik planuje przerwać pracę na dłuższy okres lub zakończyć pracę - zobowiązany jest do wyłączenia stanowiska komputerowego,
    3) stosuje się wygaszacze ekranów aktywujące się po 5 minutach od moment braku aktywności w systemie informatycznym. Ponowne rozpoczęcie pracy następuje po wprowadzeniu identyfikatora oraz hasła,
3. Zakończenie pracy na stanowisku komputerowym:
    1) Opuszczając pomieszczenie, w którym przetwarzane są informacje, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona, pracownik zobowiązany jest do zabezpieczenia pomieszczenia przed dostępem osób nieuprawnionych. Zabronione jest pozostawianie bez nadzoru pomieszczeń, w których przetwarzane są informacje.

2) Kończąc pracę w systemie informatycznym pracownik wylogowuje się ze wszystkich aplikacji, z których korzystał, wyłącza stację roboczą i zabezpiecza nośniki danych oraz dokumentację papierową.

**§ 7**
**Zasady pracy użytkowników systemu**

1. Podczas pracy na stanowisku komputerowym niedozwolone jest:
   1) podłączanie prywatnych urządzeń mobilnych (telefon, tablet, itp.) do portów USB stanowiska komputerowego,
   2) korzystanie z prywatnych nośników danych (Pendrive, płyty CD/DVD, dyski przenośne, itp.),
   3) korzystania z prywatnej poczty e-mail,
   4) w sytuacji wystąpienia konieczności odczytu informacji z nośników danych należy się zgłosić do informatyka, który wyznaczy dedykowane stanowisko do odczytu i przeniesienia danych,
   5) podejmowanie prób omijania mechanizmów zabezpieczeń i kontroli,
   6) testowanie zabezpieczeń pod kątem możliwości ich złamania,
   7) skanowanie urządzeń sieciowych, serwerów oraz stacji komputerowych pod kątem badania świadczonych usług,
   8) wyłączanie programów uruchamianych automatycznie przy starcie systemu,
   9) podejmowanie jakichkolwiek prób ingerencji w sprzęt komputerowy, poza czynnościami związanymi z codzienną eksploatacją,
   10) wyłączanie, blokowanie, odinstalowywanie zmiana parametrów oprogramowania chroniącego stanowisko komputerowe przed szkodliwym oprogramowaniem,
   11) przechowywanie na dysku lokalnym oraz w zasobie sieciowym udostępnionym użytkownikowi, dokumentów nie związanych z zakresem czynności (gier, filmów, obrazów, dźwięków),
   12) przenoszenie i przełączanie stanowisk komputerowych między stanowiskami pracy bez wiedzy informatyka,
   13) dopuszczanie do pracy na stanowisku komputerowym osób postronnych,
   14) kopiowanie i przechowywanie na stanowisku komputerowym lub nośnikach zewnętrznych danych osobowych, za wyjątkiem czynności udostępniania informacji podmiotom uprawnionym,
   15) podłączanie aktywnych urządzeń sieciowych (switch, router, access point, itp.) do gniazd sieci komputerowej.
2. Użytkownicy zgłaszają informatykowi wszelkie nieprawidłowości w działaniu stanowiska komputerowego, mogące wskazywać na zainfekowanie szkodliwym oprogramowaniem (uruchamianie się nieznanych wcześniej programów, pojawianie się nieznanych komunikatów, spowolnienie działania systemu).

**§ 8**
**Zasady korzystania z poczty elektronicznej**

1. Poczta elektroniczna znajduje się w domenie internetowej wabrzezno.pl .
2. Użytkownik konta pocztowego odpowiada za treść wysyłanych z tego konta wiadomości.
3. Użytkownik powinien:
   1) zwracać szczególną uwagę na wiadomości nieznanego pochodzenia mogące stwarzać zagrożenie bezpieczeństwa,
   2) przekazywać wg właściwości wiadomości skierowane do niewłaściwego adresata oraz poinformowanie o tym nadawcy wiadomości,
4. Informatyk konfiguruje na stanowisku komputerowym użytkownika konto pocztowe, w programie do obsługi poczty elektronicznej,
5. W przypadku wykrycia zagrożenia bezpieczeństwa systemu ze strony konta poczty elektronicznej, informatyk:
   1) blokuje konto,

2) informuje użytkownika konta o zaistniałym incydencie,
3) zabezpiecza wiadomości poczty elektronicznej dla zagrożonego konta na stanowiskach komputerowych użytkowników,
4) analizuje incydent i wprowadza zabezpieczenia minimalizujące jego powtórne wystąpienie,
5) informuje bezpośredniego przełożonego - jeżeli incydent spowodowany został przez zamierzone działanie osób trzecich.

6. użytkownicy poczty elektronicznej w stopce każdej wiadomości wpiszą informację:
**KLAUZULA POUFNOŚCI**
Ta wiadomość pocztowa i wszelkie załączone do niej pliki są poufne i podlegają ochronie prawnej. Jeśli nie jesteś jej prawidłowym adresatem, jakiekolwiek jej ujawnienie, reprodukcja, dystrybucja lub inne rozpowszechnienie, są ściśle zabronione. Jeśli otrzymał Pan/Pani niniejszy przekaz wskutek błędu, proszę o niezwłocznie powiadomienie nadawcy i usunięcie otrzymanych informacji.
7. użytkownicy podczas wysyłania wiadomości e-mail do więcej niż jednego odbiorcy korzystają z opcji „ukryta kopia”/ „UDW”.

## § 9
## Kopie zapasowe

1) Czas przechowywania danych na nośnikach elektronicznych wbudowanych w sprzęt informatyczny oraz na zewnętrznych nośnikach danych ma być niezbędny do spełnienia celu dla jakiego zostały pozyskane, a przede wszystkim zgodny z przepisami prawa. Po ustaniu czasu przechowywania zawartość nośnika podlega usunięciu.
2) Obowiązek usunięcia danych z nośnika lub jego zniszczenie spoczywa na użytkowniku.
3) Zabrania się używania i kopiowania danych na prywatne zewnętrzne nośniki pamięci takiej jak np.: pendrive, karty pamięci, płyty CD, DVD.
4) Kopie zapasowe zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania wykonywane są w celu zachowania ciągłości działania Systemu Informatycznego.
5) Za wykonywanie, przechowywanie i testowanie poprawności kopii zapasowych odpowiada informatyk.
6) Kopie zapasowe zbiorów danych i danych użytkowników
    a) przetwarzanych na serwerach baz danych i zasobach sieciowych udostępnionych użytkownikom - wykonywane są przez informatyka według ustalonego harmonogramu jako kopie codzienne (kopie online) i naprzemiennie tygodniowe (kopie offline).
    b) przetwarzanych na stanowiskach komputerowych użytkowników - wykonywane są codzienni automatycznie na nośnik sieciowy (QNAP NAS).
7) Kopie zapasowe oprogramowania systemowego

a) zainstalowanego na serwerach – wykonywane są codziennie według ustalonej godziny na nośnik sieciowy (QNAP NAS), kopie zawierają obraz systemu;
b) zainstalowanego na stanowiskach komputerowych - wykonywane są codziennie według ustalonej godziny na nośnik sieciowy (QNAP NAS), kopie zawierają obraz systemu;

8) Kopie zapasowe wykonane na nośnikach zewnętrznych przechowywane są w zamkniętym sejfie, w metalowej kasecie
9) Serwery backupowane do przynajmniej jednej lokalizacji (stref ogniowych) + dodatkowa kopia offline. Kopie zapasowe są kopiowane na odrębny serwer plików znajdujący się w innej lokalizacji (szafka sieciowa w pokoju z ograniczonym dostępem).
10) W celu zweryfikowania poprawności wykonania kopii zapasowych informatyk wykonuje testy odtwarzania.
11) Kopia zapasowa jest przechowywana w pokoju nr 28 (szafka sieciowa) i kopia

**§ 10**
**Postępowanie ze sprzętem informatycznym, nośnikami danych, naprawa, serwis sprzętu, utylizacja**

1. Przeglądy, konserwacja, naprawy oraz utylizacja sprzętu komputerowego przeprowadzane są w sposób uniemożliwiający dostęp do informacji osobom nieuprawnionym Bieżącą naprawę i konserwację sprzętu informatycznego wykonuje informatyk.
2. Prace serwisowe wykonywane w siedzibie administratora przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi informatyka lub innego wyznaczonego pracownika.
3. Poważne naprawy i konserwacja wykonywane przez personel zewnętrzny realizowane są w siedzibie administratora lub w siedzibie podmiotu wykonującego usługę jedynie po zawarciu z nim umowy o powierzenie przetwarzania danych osobowych oraz w przypadku, gdy sprzęt przekazywany jest wraz z danymi.
4. Przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt – wzór załącznik nr 4
5. Wycofany z eksploatacji sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania danych osobowych.
6. Informatyk dokumentuje wszelkie prace naprawy wykonywane przez podmioty zewnętrzne, jak i informatyka.
7. Dokumentując czynności informatyk uwzględnia następujące informacje:
    1) wskazanie osoby przeprowadzającej naprawy oraz podmiotu, którego osoba ta jest pracownikiem,
    2) wskazanie osoby nadzorującej przebieg naprawy (dotyczy sytuacji, gdy prace realizowane są w siedzibie administratora)
    3) przedmiot napraw (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu),
    4) zakres napraw,
    5) czas przeprowadzania napraw.
8. Jako elektroniczne nośniki informacji wykorzystane są w szczególności**:**
    1) pamięci masowe (dyski twarde) serwerów baz danych, serwerów plików i serwerów kopii zapasowych,
    2) pamięć typu flash

3) karty pamięci
4) płyt CD, DVD
5) oraz inne urządzenia do kopiowania i przenoszenia danych.

9. Przekazywanie urządzeń lub nośników zawierających dane osobowe, poza obszar przetwarzania danych osobowych, zabezpieczane są w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
   1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi,
   2) stosowanie metod kryptograficznych,
   3) stosowanie odpowiednich zabezpieczeń fizycznych,
   4) stosowanie odpowiednich zabezpieczeń organizacyjnych.
10. Zabronione jest wykorzystywanie prywatnych nośników danych.
11. Osoby uprawnione mają prawo wykorzystywać wyłącznie nośniki danych oraz sprzęt informatyczny przydzielony im przez administratora.
12. Ewidencjonowanie oraz wydawanie sprzętu mobilnego i elektronicznych nośników informacji dokumentowane jest przez informatyka. Nie dotyczy to płyt CD i DVD.
13. Polecenie wydania osobie uprawnionej mobilnego sprzętu informatycznego oraz elektronicznego nośnika informacji podejmuje jego bezpośredni przełożony, nie dotyczy to płyt CD i DVD.
14. Osoby uprawnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:
   1) Dane z nośników niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone.
   2) Uszkodzone nośniki należy zniszczyć fizycznie – wzór – zał. nr 5.
   3) W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych. W przypadku braku możliwości programowego usunięcia danych, dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada informatyk. Zniszczenie nośnika potwierdzane jest protokołem w skład komisji wchodzą ~~i~~nformatyk oraz użytkownik lub inna wskazana osoba - wzór – zał. nr 5.
15. Protokoły, o których mowa wyżej lub ich kopie przechowywane są przez informatyka.

## § 11
## Zasady korzystania z informatycznego sprzętu mobilnego

1. Przetwarzanie danych osobowych przy użyciu mobilnego sprzętu informatycznego powinno być ograniczone do niezbędnych przypadków. Administrator wyraża zgodę na przetwarzanie danych osobowych przy użyciu takiego rodzaju sprzętu poza strefą przetwarzania danych osobowych pracownikom, którzy zgodnie z zakresem swoich obowiązków wykonują pracę poza siedzibą administratora.
2. Administrator zakazuje użytkownikowi korzystania z publicznych dostępowych punktów HOTSPOT.
3. Administrator zobowiązuje użytkowników do wyłącznego korzystania z WiFi udostępnianego w służbowych smartfonach.
4. Hasło do tego punktu dostępowego powinno posiadać **minimum 8 znaków zawierających duże i małe litery cyfrę oraz znak specjalny**.
5. Osoba korzystająca z mobilnego sprzętu informatycznego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie

przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

6. Użytkownik mobilnego sprzętu informatycznego zobowiązany jest do:
    1) Transportu mobilnego sprzętu informatycznego w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
        a) transportowania mobilnego sprzętu informatycznego w bagażu podręcznym,
        b) nie pozostawiania mobilnego sprzętu informatycznego przechowalni bagażu oraz w widocznym miejscu w samochodzie,
        c) zaleca się przenoszenie i przewożenie mobilnego sprzętu informatycznego w torbie specjalnie do tego przeznaczonej.
    2) Korzystania z mobilnego sprzętu informatycznego w sposób minimalizujący ryzyko przejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności w miejscach publicznych i w środkach transportu publicznego.
    3) Uniemożliwienie korzystania osobom nieupoważnionym z mobilnego sprzętu informatycznego, na którym przetwarzane są dane osobowe.
    4) Ochrony sprzętu przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego mają obowiązek przestrzegać zaleceń producentów dotyczących ochrony sprzętu.
    5) Korzystania z mobilnego sprzętu informatycznego zabezpieczanego hasłem.
    6) Blokowania dostępu do mobilnego sprzętu informatycznego w przypadku gdy nie jest on wykorzystywany przez pracownika poprzez zastosowanie wygaszacza ekranu lub wylogowania z systemu.
    7) Hasło dostępu do urządzenia mobilnego typu: smartfon, tablet, terminal mobilny składa się z 4 znaków – cyfr lub wzoru.
    8) Blokada ekranu urządzenia następuje po max 30 sek. od momentu moment braku aktywności w systemie urządzenia.
    9) Hasło dostępu do urządzenia użytkownik nadaje osobiście niezwłocznie po jego otrzymaniu.
    10) użytkownik w/wym. urządzeń zobowiązany do zmiany hasła nie rzadziej niż co 12 miesięcy, chyba że zmiana hasła jest wymuszona przez system informatyczny lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby
    11) hasło powinno różnić się od poprzednio używanego,
    12) wprowadzania danych osobowych przetwarzanych na mobilnym sprzęcie informatycznym do systemu informatycznego w celu umożliwienia ich dalszego przetwarzania,
7. Przetwarzania danych przy użyciu sprzętu mobilnego jest dopuszczalne zgodnie z n/wym. zasadami:
    1) Dane przechowywane na elektronicznych nośnikach wbudowanych w sprzęt informatyczny mogą być przetwarzane do czasu spełnienia celu w jakim zostały one na nośniku zapisane.
    2) Po upływie czasu przechowywania zawartość nośnika podlega usunięciu.
    3) Obowiązek usunięcia danych z nośnika lub jego zniszczenia spoczywa na użytkowniku.
    4) Zabrania się używania i kopiowania danych na prywatne zewnętrzne nośniki pamięci takiej jak np.: pendrive, karty pamięci, płyty CD, DVD.
8. Informatyk zobowiązany jest do podjęcia działań mających na celu zabezpieczenie mobilnego sprzętu informatycznego tj. m.in. do:
    1) Konfiguracji oprogramowania w sposób wymuszający korzystanie z haseł, jeżeli system umożliwia taką konfigurację. Wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.
    2) Instalacji i konfiguracji oprogramowania antywirusowego na sprzęcie mobilnym.

9. W razie zgubienia lub kradzieży mobilnego sprzętu informatycznego pracownik zobowiązany jest do natychmiastowego powiadomienia bezpośredniego przełożonego.

**§ 12**
**Reagowanie na incydenty bezpieczeństwa oraz przywracanie sprawności działania systemu TI**

1. Informatyk odpowiada za obsługę incydentów bezpieczeństwa teleinformatycznego.
2. Po wykryciu incydentu bezpieczeństwa systemu TI, w tym działania szkodliwego oprogramowania w systemie TI:
    1) blokuje dostęp do zagrożonego stanowiska komputerowego,
    2) informuje bezpośredniego przełożonego, administratora oraz inspektora ochrony danych o zaistniałym incydencie,
    3) zabezpiecza logi systemu operacyjnego na zainfekowanym stanowisku komputerowym,
    4) zabezpiecza logi połączeń z siecią publiczną zainfekowanego stanowiska komputerowego,
    5) przywraca stanowisko komputerowe do stanu z przed incydentu,
    6) analizuje incydent i wprowadza zabezpieczenia minimalizujące jego powtórne wystąpienie,
    7) informuje bezpośredniego przełożonego lub administratora - jeżeli incydent spowodowany został przez zamierzone działanie osób trzecich,
    8) sporządza opis incydentu bezpieczeństwa zawierający:
        a) identyfikator stanowiska komputerowego (numer IP i numer inwentarzowy), na którym wykryte zostało szkodliwe oprogramowanie,
        b) dokładaną datę i czas wykrycia,
        c) rodzaj wykrytego wirusa lub innego oprogramowania,
        d) opis podjętej akcji naprawczej mającej na celu przywrócenie właściwego poziomu bezpieczeństwa.
3. W przypadku zablokowania baz danych w systemie TI podejmuje działania przywracające dostępność danych przy zastosowaniu kopii zapasowych wykonywanych w jednostce.
4. Szczegółowe zasady reagowania na incydenty związane z działaniem systemu TI opisano w załączniku nr 6.

Załączniki:

1. Wzór wykazu sprzętu informatycznego oraz oprogramowania stosowanego do przetwarzania informacji.
2. Kategorie stron internetowych (WWW) podlegających zablokowaniu lub częściowemu zablokowaniu
3. Wniosek o nadanie/cofnięcie/zmianę/zawieszenie uprawnień do przetwarzania informacji i danych osobowych w systemie informatycznym
4. Protokół przekazania sprzętu komputerowego do naprawy/serwisu/utylizacji
5. Protokół zniszczenia sprzętu komputerowego/nośnika danych
6. Procedura zarządzania incydentami z zakresu bezpieczeństwa systemów teleinformatycznych i informacji