

Zarządzenie Nr 85/2022
Wójta Gminy Kleszczewo
z dnia 30 grudnia 2022 r.

w sprawie: ustanowienia Polityki Bezpieczeństwa Informacji (PBI) w Urzędzie Gminy Kleszczewo.

Na podstawie art. 31 i 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2022 r. poz. 559 ze zm.), w związku z § 20 ust. 1 i 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla systemów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247) zarządzam, co następuje:

§ 1

Dla zapewnienia właściwej ochrony przetwarzanych danych i informacji ustanawia się Politykę Bezpieczeństwa Informacji (PBI) w Urzędzie Gminy Kleszczewo, stanowiącą załącznik do niniejszego Zarządzenia.

§ 2

Celem wprowadzenia Polityki Bezpieczeństwa Informacji (PBI) jest zapewnienie poufności, dostępności oraz integralności danych i informacji przetwarzanych w Urzędzie Gminy Kleszczewo zgodnie ze standardami określonymi w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla systemów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI).

§ 3

Zobowiązuje się wszystkich pracowników Urzędu Gminy Kleszczewo do zapoznania się i przestrzegania niniejszego Zarządzenia.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania

**POLITYKA BEZPIECZEŃSTWA INFORMACJI
URZĘDU GMINY KLESZCZEWO**

**ROZDZIAŁ I
PRZEPISY OGÓLNE**

§ 1

1. Polityka Bezpieczeństwa Informacji, zwana dalej „Polityką”, określa podstawowe zasady zarządzania bezpieczeństwem informacji oraz komórki organizacyjne odpowiedzialne za ochronę informacji w Urzędzie Gminy Kleszczewo, zwanym dalej „Urzędem”.
2. Zasady zarządzania bezpieczeństwem informacji w Urzędzie Gminy Kleszczewo zostały opracowane zgodnie z obowiązującymi przepisami w oparciu o wymagania Polskich Norm i standardów w obszarze bezpieczeństwa informacji, w tym w szczególności:
 - 1) rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016r. 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) (Dz. Urz. UE L z 2016 r. Nr 119), zwanym dalej „RODO”;
 - 2) ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. (t.j. Dz. U. z 2019 r. 1781);
 - 3) ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U.2022 r. 902);
 - 4) ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. 2019 r. 749 ze zm);
 - 5) ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U.2022 r. 1863);
 - 6) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U.2021 r. poz. 207 ze zm);
 - 7) Rozporządzeniem Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (t.j. Dz.U. 2017 r. poz. 2247)
 - 8) 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 (t.j. Dz.U. z 2017 r. poz. Nr 2247);
 - 9) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (t.j. Dz.U. z 2007 r. Nr 10, poz. 68).

§ 2

Użyte w Polityce pojęcia oznaczają:

- 1) aktywa (*zasoby*) - wszystko, co stanowi wartość dla Urzędu i w związku z tym wymaga ochrony, w szczególności aktywa informacyjne (*informacje*) rozumiane jako wiedza, dane oraz wszelkie informacje wpływające na wartość Urzędu, w tym informacje udokumentowane;
- 2) zasoby ludzkie - pracownicy, wiedza, umiejętności, doświadczenie i kwalifikacje, usługi i licencje, wartości niematerialne, w tym wizerunek, kultura organizacyjna, wartości etyczne, systemy teleinformatyczne i cyberbezpieczeństwo Urzędu, urządzenia dostępne i oprogramowanie, zabezpieczenia fizyczne, środowiskowe, techniczne i organizacyjne,

- siedziba i nieruchomości oraz poszczególne pomieszczenia użytkowane przez Urząd;
- 3) bezpieczeństwo informacji - zabezpieczenie i zachowanie informacji w zakresie integralności, dostępności i poufności przed nieautoryzowanym dostępem lub zmianą; dodatkowo mogą być brane pod uwagę inne atrybuty - rozliczalność, autentyczność, niezaprzeczalność oraz niezawodność;
 - 4) dostępność - właściwość polegająca na tym, że informacja jest dostępna i użyteczna na żądanie upoważnionego podmiotu;
 - 5) gestor systemu - kierownik komórki organizacyjnej teleinformatyki Urzędu lub inna, wskazana osoba, odpowiedzialna za zainicjowanie powstania systemu;
 - 6) incydent związany z bezpieczeństwem informacji - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które zagrażają bezpieczeństwu informacji oraz stwarzają znaczne prawdopodobieństwo utraty aktywów lub zakłócenia realizacji zadań;
 - 7) integralność - właściwość polegająca na zapewnieniu dokładności i kompletności informacji;
 - 8) podatność - słabość lub wrażliwość aktywa lub grupy aktywów w zakresie funkcjonowania Urzędu, która może wpłynąć na wystąpienie zagrożenia i jego ewentualne skutki; podatność może dotyczyć, w szczególności sposobu zarządzania lub postępowania, personelu, zależności, relacji, kontaktów wewnętrznych i zewnętrznych, czynnika technologicznego, niedoskonałości zabezpieczeń;
 - 9) poufność - właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
 - 10) ryzyko - potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów, powodując w ten sposób naruszenie poufności, integralności, dostępności lub innych atrybutów bezpieczeństwa informacji;
 - 11) sytuacja awaryjna - zdarzenie, którego skutki powodują utratę ciągłości działania Urzędu; może dotyczyć jednej lub kilku komórek organizacyjnych, których procesy zostały zakłócone;
 - 12) sytuacja kryzysowa - niespodziewane i niepożądane zdarzenie lub seria zdarzeń związanych z bezpieczeństwem przetwarzania informacji, w szczególności w systemach teleinformatycznych, które mogą zakłócić lub zakłócają proces realizacji zadań Urzędu (*sytuacja może dotyczyć w szczególności bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołując znaczne ograniczenia w funkcjonowaniu Urzędu*);
 - 13) SZBI - System Zarządzania Bezpieczeństwem Informacji, stanowiący część systemu zarządzania odnoszący się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji, obejmujący strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i aktywa;
 - 14) użytkownik - pracownik, stażysta, praktykant lub inna osoba wykonująca pracę bądź świadcząca usługi na podstawie umów cywilnoprawnych na rzecz Urzędu, która uzyskała upoważnienie lub powierzenie do przetwarzania danych osobowych w danym zakresie, w tym do przetwarzania informacji w systemach teleinformatycznych;
 - 15) zabezpieczenie - działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia zagrożenia lub minimalizuje jego negatywne skutki oraz wpływa na osiągnięcie celów; wyróżnia się trzy rodzaje zabezpieczeń funkcjonujących w Urzędzie ;
 - a) organizacyjne (*struktury organizacyjne, polityki, procedury postępowania, zarządzenia, regulaminy, klauzule w umowach, zakresy obowiązków pracowników, szkolenia, audyty, kontrole itp.*);
 - b) techniczne (*systemy bezpieczeństwa teleinformatycznego, systemy kontroli dostępu, ewidencje kluczy, urządzenia alarmowe, sygnalizacyjne lub monitoringu, oprogramowanie*

antywirusowe itp.);

- c) fizyczne (*pracownicy ochrony, kontrola dostępu, drzwi, pomieszczenia plombowane, zamykane szafy, sejfy, strefy ochronne, monitoring itp.*) i środowiskowe (*np. bezpieczeństwo okablowania, klimatyzacja*);

16) zagrożenie - zdarzenie, zjawisko, działanie lub zaniechanie, które może skutkować naruszeniem integralności, dostępności, poufności informacji albo doprowadzić do szkody lub nieosiągnięcia celów Urzędu.

§ 3

1. Polityka jest integralną częścią dokumentacji SZBI.
2. Polityką objęte są wszystkie informacje wykorzystywane przez Urząd, niezależnie od formy i nośnika przetwarzania lub dystrybucji (*ustne, pisemne, wizyjne, nagrania audio i wideo*), utrwalone na nośnikach elektronicznych, systemach komputerowych oraz wytworzone w dokumentach, będące własnością Urzędu oraz powierzone w ramach umów lub porozumień z kontrahentami lub wykonawcami.
3. Zapisy Polityki należy uwzględniać w procesie opracowania pozostałej dokumentacji SZBI, w szczególności procedur, instrukcji i wytycznych obowiązujących w Urzędzie.
4. Obowiązujące w Urzędzie regulacje wewnętrzne należy procedować i wdrażać z uwzględnieniem założeń zapewniających ochronę aktywów, w szczególności aktywów informacyjnych.
5. Polityka nie ingeruje w treść dokumentów dedykowanych dla systemów zarządzania bezpieczeństwem informacji, certyfikowanych na zgodność z Polską Normą PN-ISO/IEC 27001, które funkcjonują lub mogą funkcjonować w Urzędzie, a także w treść dokumentów wynikających z przepisów o ochronie informacji niejawnych.
6. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z Polityki, stosuje się przepisy tych ustaw.

§ 4

Polityka ma zastosowanie do wszystkich komórek organizacyjnych Urzędu i obejmuje zakresem nie tylko obszar Urzędu, ale także miejsca i sytuacje, w których informacje związane z działalnością Urzędu są przetwarzane poza jego siedzibą, w szczególności w kontekście zdalnego korzystania z sieci komputerowej Urzędu.

§ 5

1. Do przestrzegania Polityki zobowiązane są wszystkie osoby korzystające z zasobów Urzędu, w szczególności:
 - 1) pracownicy Urzędu;
 - 2) osoby świadczące usługi, realizujące dostawy oraz wykonujące pracę na rzecz Urzędu na podstawie umów cywilnoprawnych, w tym umów zlecenia;
 - 3) osoby odbywające praktykę lub staż, w zakresie określonym odpowiednio w umowie o odbywaniu praktyki lub stażu, programie praktyki lub stażu;
 - 4) pracownicy podmiotów zewnętrznych realizujący inne niż określone w pkt 1-3 zadania na rzecz Urzędu.
2. Za zapoznanie z Polityką osób, o których mowa w ust. 1, odpowiada w przypadku:
 - 1) nowo zatrudnionego pracownika – Inspektor Ochrony Danych;
 - 2) pracowników wykonujących obowiązki wynikające ze stosunku pracy na rzecz Urzędu, zatrudnionych na samodzielnych stanowiskach – Inspektor Ochrony Danych;
 - 3) pracowników wykonujących obowiązki wynikające ze stosunku pracy na rzecz Urzędu - kierownik komórki organizacyjnej Urzędu, w której są zatrudnieni;
 - 4) osób świadczących usługi, realizujących dostawy oraz wykonujących pracę na rzecz Urzędu na

- podstawie umów cywilnoprawnych - kierownik lub zastępca kierownika komórki organizacyjnej Urzędu odpowiedzialny za realizację umowy;
- 5) stażystów, praktykantów - kierownik lub zastępca kierownika komórki organizacyjnej Urzędu, w której będą odbywać staż lub praktykę.
3. Osoby, o których mowa w ust. 1, zobowiązane są do złożenia oświadczenia o zapoznaniu się z treścią Polityki, zgodnie z wzorem stanowiącym załącznik do Polityki.

ROZDZIAŁ II

ZASADY DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI

§ 6

1. Polityka realizowana jest w Urzędzie poprzez:
 - 1) zapewnienie odpowiedniej jakości procesów przetwarzania informacji, w szczególności skuteczności i adekwatności działania zabezpieczeń (*lub ich grup*) i środków chroniących przed nieuprawnionym ujawnieniem, odpowiednich warunków do ich użytkowania oraz sprawności i efektywności ich wykorzystywania;
 - 2) pracowników posiadających odpowiednią wiedzę, umiejętności i doświadczenie adekwatne do powierzonych zadań;
 - 3) ochronę fizyczną, techniczną i organizacyjną aktywów Urzędu przed dostępem osób nieupoważnionych, w szczególności przed nieuprawnionym wykorzystaniem, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją lub zniszczeniem;
 - 4) zabezpieczenie systemów teleinformatycznych eksploatowanych w Urzędzie przed zagrożeniami;
 - 5) zabezpieczenie aktywów w Urzędzie przed ich uszkodzeniem lub zniszczeniem w wyniku pożaru, zalania, ataku terrorystycznego, zjawisk naturalnych lub innych zagrożeń;
 - 6) zapewnienie ciągłości działania procesów przetwarzania informacji w Urzędzie;
 - 7) zapewnienie możliwości sprawnego odtworzenia aktywów w przypadku ich zniszczenia;
 - 8) zapewnienie gotowości do reakcji na sytuację awaryjną lub kryzysową;
 - 9) zapewnienie rozwiązań organizacyjnych i systemowych regulujących zasady i sposób zarządzania bezpieczeństwem informacji;
 - 10) zapewnienie spójnej polityki informacyjnej w Urzędzie;
 - 11) zapewnienie właściwych postanowień w zakresie bezpieczeństwa informacji, w szczególności stosowanie klauzul poufności w umowach cywilnoprawnych z kontrahentami lub wykonawcami;
 - 12) zapewnienie pracownikom szkoleń i innych akcji promocyjno-edukacyjnych z zakresu bezpieczeństwa informacji;
 - 13) zapewnienie działań kontrolnych w zakresie przestrzegania zasad określonych w Polityce;
 - 14) przestrzeganie zasad bezpieczeństwa informacji, o których mowa w § 10.
2. Stosowanie zabezpieczeń lub ich grup powinno uwzględniać następujące zasady:
 - 1) zabezpieczenia powinny być adekwatne do wymogów prawnych oraz wyników audytów i analiz ryzyka bezpieczeństwa informacji;
 - 2) zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie (*grupy zabezpieczeń*), zapewniając wymagany poziom bezpieczeństwa informacji; w doborze zabezpieczeń należy kierować się w szczególności:
 - a) adekwatnością,

- b) zaleceniami Polskiej Normy PN-ISO 27002,
 - c) uwzględnieniem wyników szacowania ryzyka;
- 3) świadomość pracowników w zakresie bezpieczeństwa informacji powinna być doskonała, w szczególności poprzez różne formy podnoszenia kwalifikacji;
 - 4) powinno się unikać niepotrzebnego dublowania zabezpieczeń, przy uwzględnieniu racjonalnego gospodarowania środkami publicznymi, optymalizacji potrzeb oraz ograniczeń i uwarunkowań prawno-organizacyjnych Urzędu;
 - 5) należy podejmować działania na rzecz utrzymania standardów współpracy Urzędu z osobami i podmiotami zewnętrznymi, poprzez stosowanie zasad regulujących kwestie poufności w ramach realizacji umów, porozumień, listów intencyjnych i innych form relacji, obowiązujących strony również po ustaniu współpracy.
3. Szczegółowe metody i sposoby implementacji zabezpieczeń, o których mowa w ust.1, mogą być określone w innych dokumentach stanowiących dokumentację SZBI.

§ 7

1. Skuteczność SZBI zachowuje się przy jednoczesnym zastosowaniu i uzupełnianiu się elementów regulujących obszary bezpieczeństwa fizycznego i środowiskowego, technicznego, organizacyjnego.
2. Poziom bezpieczeństwa informacji jest odpowiedni wówczas, gdy spełnione są następujące warunki:
 - 1) dokonano szacowania ryzyka w odniesieniu do bezpieczeństwa informacji;
 - 2) wdrożono skuteczne zabezpieczenia wymagane przepisami prawa i Polityką.

§ 8

1. W Urzędzie stosuje się w szczególności następujące zasady dotyczące bezpieczeństwa informacji:
 - 1) wiedzy koniecznej (*ograniczonego dostępu do informacji*) - pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań; zasada ta dotyczy głównie informacji wrażliwych; zasada ta ma ograniczone znaczenie dla pewnych grup informacji, w szczególności informacji dostępnych publicznie;
 - 2) indywidualnej odpowiedzialności - za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień; zasada ta dotyczy np. wydruków z systemu centralnego wydruku;
 - 3) niewygody uzasadnionej - bezpieczeństwo co do zasady opiera się na ograniczeniach oraz jest niewygodne; środki ochrony nie mogą nadmiernie utrudniać realizacji celów i zadań Urzędu;
 - 4) czystego biurka;
 - 5) przechowywania dokumentów w odpowiednio zabezpieczonych meblach biurowych lub szafach metalowych/sejfach;
 - 6) na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy wyłączenia komputera;
 - 7) separacji obowiązków - pojedyncze osoby nie mogą wykonywać krytycznych zadań w całości;
 - 8) dyskrekcji (*ograniczonego zaufania i odpowiedzialnej konwersacji*) - wszelkie informacje służbowe mogą być przekazywane wyłącznie w celu wykonywania zadań w zakresie do tego niezbędnym oraz osobom uprawnionym do pozyskania tych informacji; zasada ta ma ograniczone znaczenie dla pewnych grup informacji, np. informacji dostępnych publicznie;
 - 9) obecności koniecznej - prawo przebywania w określonych miejscach - istotnych dla

bezpieczeństwa informacji - powinny mieć tylko osoby upoważnione;

- 10) zamykania pomieszczeń - niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu; na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba powinna zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia;
 - 11) nadzorowania dokumentów - po godzinach pracy wszystkie dokumenty zawierające informacje podlegające ochronie powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;
 - 12) stałej gotowości - niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających system funkcjonujący w Urzędzie bez zastosowania alternatywnych mechanizmów; system powinien być sprawny i przygotowany na zidentyfikowane zagrożenia;
 - 13) zachowania prywatności kont w systemach - każdy pracownik zobowiązany jest do pracy w systemach teleinformatycznych na przypisanych lub udostępnionych mu kontach; zabronione jest udostępnianie własnych kont osobom trzecim;
 - 14) poufności haseł - każdy pracownik zobowiązany jest do zachowania poufności udostępnionych mu haseł i kodów dostępu, w szczególności do systemów teleinformatycznych;
 - 15) legalnego oprogramowania - na stacjach roboczych zainstalowane jest wyłącznie legalne oprogramowanie umożliwiające automatyczne aktualizacje;
 - 16) zgłaszania incydentów bezpieczeństwa informacji - każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu bezpieczeństwa informacji;
 - 17) automatyzacji backupu - procesy tworzenia kopii zapasowych powinny być zautomatyzowane oraz niemożliwe do przerwania przez pracownika;
 - 18) ochrony nośników danych - dane kopiowane na nośniki i wynoszone poza Urząd powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania, co najmniej poprzez szyfrowanie;
 - 19) adekwatności zabezpieczeń - używane mechanizmy zabezpieczeń powinny być adekwatne do zagrożeń, podatności, wartości aktywów oraz innych istotnych okoliczności;
 - 20) kompleksowości ochrony (*asekuracji zabezpieczeń*) - ochrona aktywów systemu przetwarzania informacji powinna opierać się na stosowaniu różnych mechanizmów ochrony, w tym ochrony: prawnej, fizycznej, technicznej oraz organizacyjnej;
 - 21) ochrony niezbędnej - minimalny wymagany poziom bezpieczeństwa informacji wynika z obowiązujących przepisów prawa; zastosowanie wyższych poziomów bezpieczeństwa informacji uzasadniają szczególne potrzeby Urzędu i wyniki szacowania ryzyka;
 - 22) bezpiecznej współpracy z podmiotami zewnętrznymi - dokumenty regulujące współpracę powinny zawierać stosowne klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu dokumentacji po ich wykorzystaniu;
 - 23) ewolucji - SZBI jest stale monitorowany i dostosowywany do zmieniających się warunków wewnętrznych i zewnętrznych;
 - 24) podwyższonego poziomu ochrony zbiorów informacji - w szczególnie uzasadnionych przypadkach zbiór informacji powinien być bardziej chroniony niż poszczególne informacje, które się na niego składają;
 - 25) czystego kosza - dokumenty papierowe, z wyjątkiem materiałów publicznie dostępnych, powinny być niszczone w sposób uniemożliwiający ich odczytanie.
2. Katalog zasad, o których mowa w ust. 1, jest otwarty i może być rozszerzony lub uszczegółowiony w innych dokumentach stanowiących dokumentację SZBI.

ROZDZIAŁ III

ODPOWIEDZIALNOŚĆ I UPRAWNIENIA W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

§ 9

1. Właściwe zarządzanie bezpieczeństwem informacji w Urzędzie zapewnia wewnętrzna struktura organizacyjna, w której skład wchodzi, w szczególności:
 - 1) Wójt;
 - 2) Zastępcy Wójta/Sekretarz Gminy;
 - 3) Skarbnik Gminy;
 - 4) Inspektor Ochrony Danych;
 - 5) Osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;
 - 6) Pełnomocnik do spraw ochrony informacji niejawnych;
 - 7) Kierownicy komórek organizacyjnych Urzędu;
 - 8) Użytkownicy.
2. Odpowiedzialność za bezpieczeństwo informacji w Urzędzie ponoszą wszystkie osoby, o których mowa w § 10 ust. 1, w zakresie odpowiednim do nałożonych na nich obowiązków, posiadanych uprawnień lub zapisów określonych w umowach, porozumieniach i innych pisemnych formach współpracy regulujących obszar bezpieczeństwa informacji.
3. Niezależnie od zakresu, o którym mowa w ust. 2, pracownicy są zobowiązani do przestrzegania obowiązku zachowania tajemnicy pracodawcy zgodnie z obowiązującymi przepisami prawa.

§ 10

1. Wójt:
 - 1) decyduje o celach i środkach przetwarzania informacji, w tym danych osobowych, jako ich administrator;
 - 2) ustanawia Politykę oraz SZBI;
 - 3) wyznacza lub powołuje:
 - a) Inspektora Ochrony Danych,
 - b) Pełnomocnika do spraw Ochrony Informacji Niejawnych,
 - c) osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
2. Zastępca Wójta/Sekretarz Gminy:
 - 1) wstępnie akceptuje wyniki przeglądów zarządzania bezpieczeństwem informacji oraz raporty z incydentów bezpieczeństwa;
 - 2) określa kierownikom komórek organizacyjnych Urzędu zadania mające na celu zapewnienie bezpieczeństwa informacji, w przypadku wystąpienia takiej potrzeby;
 - 3) egzekwuje odpowiedzialność pracowników Urzędu za naruszenia związane z bezpieczeństwem informacji, w zakresie adekwatnym do nałożonych na nich obowiązków i posiadanych uprawnień.
3. Zadania Inspektora Ochrony Danych określa art. 39 RODO.
4. Osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa realizuje zadania wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym

systemie cyberbezpieczeństwa.

5. Pełnomocnik do spraw Ochrony Informacji Niejawnych realizuje zadania wynikające z ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych.
6. Kierownicy komórek organizacyjnych Urzędu, w zakresie swojej właściwości, odpowiadają za:
 - 1) wdrożenie i przestrzeganie Polityki;
 - 2) ochronę aktywów;
 - 3) realizację procedur zapewniających ciągłość funkcjonowania komórki w sytuacjach awaryjnych i kryzysowych;
 - 4) umożliwienie pracownikom udziału w organizowanych szkoleniach z zakresu bezpieczeństwa informacji;
 - 5) właściwy tryb zgłaszania, postępowania i dokumentowania incydentów, zgodnie z wewnętrznymi regulacjami w tym zakresie.
7. Użytkownicy odpowiadają w szczególności za:
 - 1) przestrzeganie Polityki;
 - 2) ochronę aktywów, w zakresie swojej właściwości;
 - 3) niezwłoczne reagowanie w przypadku wystąpienia lub podejrzenia wystąpienia incydentu oraz postępowanie zgodnie z wewnętrznymi regulacjami w tym zakresie;
 - 4) zabezpieczanie informacji przed ich udostępnieniem osobom nieupoważnionym, zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem;
 - 5) zachowanie w tajemnicy informacji pozyskanych w ramach wykonywania obowiązków służbowych w Urzędzie oraz przestrzegania zasad bezpiecznego ich przetwarzania, w tym w systemach teleinformatycznych, w zakresie nadanych uprawnień lub wskazanym w upoważnieniu do przetwarzania danych osobowych.

ROZDZIAŁ IV

KLASYFIKACJA INFORMACJI I ZASADY POSTĘPOWANIA Z INFORMACJAMI

§ 11

1. W Urzędzie przyjmuje się następującą klasyfikację informacji oraz ich oznaczenie:
 - 1) informacje publiczne - informacje, których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej;
 - 2) informacje udostępniane w szczególności na stronach internetowych Urzędu;
 - 3) informacje prawnie chronione;
 - 4) informacje stanowiące dane osobowe podlegające ochronie na mocy przepisów o ochronie danych osobowych;
 - 5) informacje przekazane Urzędowi przez kontrahenta, co do których podjął on działania w celu zachowania ich w poufności, w szczególności nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą (*tajemnica przedsiębiorstwa*);
 - 6) informacje przekazane Urzędowi przez mieszkańca, co do których podjął on działania w celu zachowania ich w poufności, w szczególności nieujawnione do wiadomości publicznej naruszające dobra osobiste;
 - 7) informacje chronione na mocy ustawy o ochronie informacji niejawnych (*uregulowane odrębnymi przepisami*);

- 8) informacje wewnętrzne Urzędu, wytworzone w Urzędzie lub na jego rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup. Są to informacje ogólnie dostępne wewnątrz Urzędu oraz przeznaczone do użytku wewnętrznego.
2. Wprowadzenie klasyfikacji informacji, o której mowa w ust. 1, nie powoduje konieczności specjalnego fizycznego oznaczania informacji udokumentowanych, dokonuje się w nich jedynie odwzorowania literowo-cyfrowego zgodnie z instrukcją kancelaryjną lub oznaczenia identyfikującego dokument.
3. W Urzędzie przyjmuje się następujące zasady postępowania z informacjami:
 - 1) informacja publiczna - przetwarzanie, przechowywanie, przekazywanie w sposób gwarantujący zachowanie integralności i dostępności informacji. Zmiana klasyfikacji i udostępnianie na zasadach i w trybie przewidzianym przepisami prawa. Niszczenie zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Urząd umowach oraz Instrukcją kancelaryjną;
 - 2) informacja prawnie chroniona - przetwarzanie w sposób gwarantujący zapewnienie bezpieczeństwa informacji ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności oraz innych atrybutów bezpieczeństwa, które są wymagane dla danej informacji chronionej na podstawie właściwej ustawy. Przechowywanie w sposób gwarantujący zapewnienie bezpieczeństwa informacji. Przekazywanie wyłącznie osobom uprawnionym, w sposób gwarantujący zachowanie integralności i poufności oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Urząd umowach. Zmiana klasyfikacji zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Urząd umowach. Udostępnianie wyłącznie uprawnionym osobom lub podmiotom po uzyskaniu zgody administratora danych. Niszczenie zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Urząd umowach;
 - 3) informacja szczególna - przetwarzanie w sposób gwarantujący zapewnienie bezpieczeństwa informacji, ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności. Przechowywanie w sposób gwarantujący zapewnienie bezpieczeństwa informacji. Przekazywanie wyłącznie osobom uprawnionym (*pracownikom, osobom, z którymi Urząd zawarł stosowne umowy*), w sposób gwarantujący zachowanie integralności i dostępności informacji oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Urząd umowach. Zmiana klasyfikacji możliwa po podjęciu decyzji przez uprawnione osoby oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Urząd umowach. Udostępnianie wyłącznie po uzyskaniu zgody administratora danych. Niszczenie zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Urząd umowach oraz instrukcją kancelaryjną;
 - 4) informacja wymagająca klasyfikacji - przetwarzanie gwarantujące zachowanie integralności, dostępności i poufności informacji. Przechowywanie w sposób gwarantujący zapewnienie bezpieczeństwa informacji. Przekazywanie możliwe wysyłanie adresatom zewnętrznym po dokonaniu analizy prawnej dotyczącej możliwości udostępnienia informacji oraz analizy ewentualnych konsekwencji z tym związanych. Przekazywanie wewnątrz Urzędu na zasadach określonych przez kierownika właściwej komórki organizacyjnej. Zmiana klasyfikacji po dokonaniu analizy w tym zakresie. Udostępnianie wyłącznie po uzyskaniu zgody administratora danych. Niszczenie zgodnie z instrukcją kancelaryjną.
4. Klasyfikacja informacji w systemach teleinformatycznych, w których ustanowiono SZBI certyfikowany za zgodność z normą PN-ISO/IEC 27001, odbywa się w trybie przewidzianym w dokumentacji tego systemu.

ROZDZIAŁ V

SZACOWANIE RYZYKA

§ 12

1. W obszarze bezpieczeństwa informacji identyfikacja i analiza ryzyka jest obligatoryjna i przeprowadza się ją cyklicznie, nie rzadziej niż raz w roku.
2. Identyfikacja i analiza ryzyka powinna być dodatkowo realizowana zgodnie z potrzebami, w szczególności przed opracowaniem dokumentacji bezpieczeństwa dla danego obszaru lub systemu oraz po wystąpieniu istotnych zmian w danym obszarze lub systemie.
3. Identyfikację i analizę ryzyka przeprowadza się w oparciu o dostępne metodyki.
4. Identyfikacja i analiza ryzyka powinna być udokumentowana.
5. Identyfikacja i analiza ryzyka w systemach teleinformatycznych, w których ustanawiano SZBI certyfikowany za zgodność z Polską Normą PN-ISO/IEC 27001, odbywa się w trybie przewidzianym w dokumentacji tego systemu.

ROZDZIAŁ VI

POSTANOWIENIA KOŃCOWE

§ 13

1. Dokumentacja z zakresu bezpieczeństwa informacji, o której mowa w § 3 ust. 3, jest wprowadzana odrębnymi regulacjami.
2. W terminie 30 dni od dnia wejścia w życie Polityki osoby, o których mowa w § 5, mają obowiązek zapoznać się z jej treścią.

**Załącznik
do Polityki Bezpieczeństwa
Informacji Urzędu Gminy
Kleszczewo**

**Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji
w Urzędzie Gminy Kleszczewo.**

Niniejszym oświadczam, że zapoznałam/em się z Polityką Bezpieczeństwa Informacji (PBI) w Urzędzie Gminy Kleszczewo i zobowiązuję się do przestrzegania zawartych w niej zasad.

Mam na uwadze zachowanie w tajemnicy informacji prawnie chronionych, do których mam lub będę miał/a dostęp w związku z wykonywaniem przeze mnie obowiązków pracowniczych lub innych wykonywanych na rzecz Urzędu Gminy Kleszczewo, a także sposobów zabezpieczenia tych informacji, zarówno w trakcie wykonywania zadań, jak i po ich zakończeniu.

Mam świadomość, że celem Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Kleszczewo jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji przetwarzanych w Urzędzie Gminy Kleszczewo, a naruszenia związane z bezpieczeństwem informacji mogą skutkować odpowiedzialnością karną lub dyscyplinarną na zasadach i w trybie przewidzianym w przepisach prawa, w tym ustawie z dnia z dnia 26 czerwca 1974 r. - Kodeks pracy (t.j. Dz.U.2022 r . poz. 1510).

data i czytelny podpis