WÓJT GMINY
CHRZYPSKO WIELKIE
ul. Główna 15
64-412 Chrzypsko Wielkie

SA.0050.43.2026

Zarządzenie Nr 43/2026

Wójta Gminy Chrzypsko Wielkie

z dnia 15 września 2026 r.

w sprawie aktualizacji dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania w Urzędzie Gminy Chrzypsko Wielkie

Na podstawie art. 30 ust. 1 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, w związku z art. 8 ust. 3 i 4, art. 8c-8f, art. 9-12c oraz art. 16d-16h ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20, 252, 815, z późn. zm.), z uwzględnieniem wymagań Załącznika nr 4 do tej ustawy oraz § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zarządzam, co następuje:

§ 1.

1. Z dniem 15 września 2026 r. zatwierdza się i wprowadza zaktualizowane wersje 0.2 następujących dokumentów Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania:
   a) Polityka Bezpieczeństwa Informacji i Ciągłości Działania - Załącznik nr 1;
   b) Procedura zarządzania incydentami w Urzędzie Gminy Chrzypsko Wielkie - Załącznik nr 2;
   c) Procedura zarządzania ryzykiem: identyfikacja, analiza i ocena ryzyk oraz postępowanie z ryzykiem w obszarze bezpieczeństwa informacji i ciągłości działania - Załącznik nr 3;
   d) Procedury bezpieczeństwa fizycznego, technicznego i środowiskowego - Załącznik nr 4;
   e) Zasady bezpieczeństwa informacji w relacjach z dostawcami - Załącznik nr 5;
   f) Zasady klasyfikacji informacji i postępowania z informacjami - Załącznik nr 6.
2. Wszystkie dokumenty, o których mowa w ust. 1, posiadają oznaczenie „wersja 0.2" oraz datę zatwierdzenia 15 września 2026 r.

§ 2.

1. Aktualizacja dokumentacji uwzględnia w szczególności:
   a) ustawowy zakres SZBI dla podmiotu ważnego będącego podmiotem publicznym;
   b) odpowiedzialność i obowiązki kierownika podmiotu;
   c) wymagania dotyczące osób realizujących zadania z art. 8 lub art. 11 ustawy o KSC;
   d) obowiązki szkoleniowe;
   e) aktualne zasady obsługi i zgłaszania incydentów poważnych;

f) wymagania dotyczące ochrony fizycznej, dostawców, kopii zapasowych, cyberhigieny, zarządzania uprawnieniami i dokumentowania działań;
g) a także możliwość wspólnego wykonywania obowiązków z zakresu cyberbezpieczeństwa przez podmioty publiczne.

2. Za koordynację wdrożenia zaktualizowanej dokumentacji w Urzędzie odpowiada Pełnomocnik ds. Bezpieczeństwa Informacji i Ciągłości Działania we współpracy z osobami funkcyjnymi wskazanymi w dokumentacji SZBI i CD.

§ 3.

1. Kierownicy jednostek organizacyjnych Gminy Chrzypsko Wielkie, które spełniają przesłanki uznania za podmiot ważny, w szczególności na podstawie art. 5 ust. 2 pkt 8 ustawy o KSC, w tym odpowiednio samorządowych jednostek budżetowych, samorządowych zakładów budżetowych, samorządowych instytucji kultury oraz spółek wykonujących zadania o charakterze użyteczności publicznej, jeżeli realizują zadania publiczne z wykorzystaniem systemów informacyjnych, zapewniają wykonanie obowiązków wynikających z ustawy o KSC w kierowanych jednostkach, w tym wdrożenie i utrzymywanie właściwego SZBI zgodnego z Załącznikiem nr 4 do ustawy o KSC oraz realizację obowiązków kierownika podmiotu określonych w art. 8c-8e tej ustawy.
2. Jednostki organizacyjne mogą stosować dokumenty, o których mowa w § 1, po ich formalnym wprowadzeniu w danej jednostce albo w zakresie wynikającym z ustanowionej wspólnej obsługi cyberbezpieczeństwa.
3. W przypadku ustanowienia wspólnej obsługi albo jednostki wyznaczonej zgodnie z art. 16e-16h ustawy o KSC, kierownicy jednostek objętych wspólną obsługą zapewniają współpracę z jednostką wyznaczoną, w szczególności terminowe przekazywanie informacji o incydentach oraz wykonywanie decyzji dotyczących SZBI w zakresie przewidzianym przepisami i przyjętym modelem obsługi.

§ 4.

1. Z dniem wejścia w życie niniejszego Zarządzenia tracą moc wcześniejsze wersje dokumentów wymienionych w § 1, w tym wersje wprowadzone Zarządzeniem Nr 93/2024 Wójta Gminy Chrzypsko Wielkie z dnia 30 grudnia 2024 r., w zakresie zastąpionym załącznikami do niniejszego Zarządzenia.
2. Pozostałe postanowienia Zarządzenia Nr 93/2024, w szczególności dotyczące powołania Komitetu Bezpieczeństwa i jego składu, pozostają w mocy, o ile nie są sprzeczne z niniejszym Zarządzeniem.

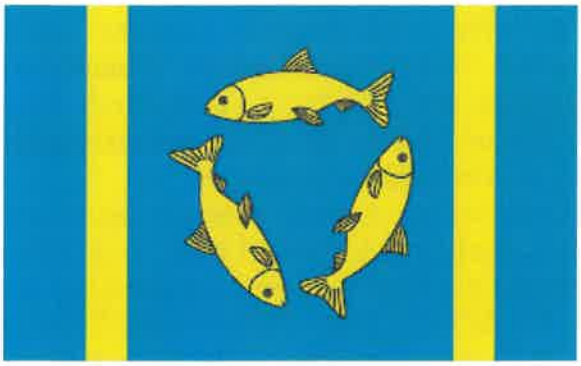
§ 5.

Pełnomocnik ds. Bezpieczeństwa Informacji i Ciągłości Działania zapewnia przekazanie zaktualizowanej dokumentacji pracownikom Urzędu, udokumentowanie zapoznania się z nią w zakresie adekwatnym do pełnionych obowiązków oraz włączenie zmian do programu szkoleń i budowy świadomości cyberbezpieczeństwa.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

Wójt
mgr inż. Edmund Ziółek



DOKUMENT SYSTEMU ZARZĄDZANIA

BEZPIECZEŃSTWEM INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

Polityka Bezpieczeństwa Informacji i Ciągłości Działania w Urzędzie Gminy Chrzypsko Wielkie

Nazwa dokumentu	**Polityka bezpieczeństwa informacji i ciągłości działania**
Autor dokumentu	Joanna Mrowicka
Sprawdzająca dokument	Aneta Skrzypczak-Kurzawa
Wersja dokumentu	0.2
Zatwierdzający dokument	Wójt Gminy
Data zatwierdzenia dokumentu	15 września 2026r.

I. Postanowienia ogólne

1. Informacja jest jednym z podstawowych, krytycznych zasobów Urzędzie Gminy Chrzypsko Wielkie (zwanego dalej Urzędem Gminy lub Urzędem). Konieczność zapewnienia jej odpowiedniego bezpieczeństwa jest jednym z nadrzędnych zadań Urzędu, uwzględniając, że Urząd Gminy posiada dostęp do informacji szczególnie wrażliwych – zawartych przede wszystkim w dokumentacji urzędowej.
2. Zarządzanie bezpieczeństwem informacji odbywa się zgodnie z przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20, 252, 815, z późn. zm.), w szczególności art. 8 ust. 3 i 4 oraz Załącznikiem nr 4 do tej ustawy. Normy PN-ISO/IEC 27001, PN-ISO/IEC 27002 i PN-ISO/IEC 27005 są stosowane jako metodyka uzupełniająca, o ile nie pozostaje ona w sprzeczności z wymaganiami ustawowymi.
   1) PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń;
   2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem.
3. Domeny bezpieczeństwa, jak bezpieczeństwo fizyczne, środowiskowe, techniczne czy osobowe w Systemie Zarządzania Bezpieczeństwem Informacji i Ciągłością Działania (dalej: SZBI i CD) nie są celami samymi w sobie a jedynie środkami, do osiągnięcia ostatecznego celu jakim jest zapewnienie bezpieczeństwa informacji oraz właściwej ciągłości działania w ramach świadczonych usług publicznych.
4. Kierownictwo Urzędu Gminy jest świadome, że zachowanie poufności, integralności, dostępności oraz autentyczności informacji przetwarzanych w Urzędzie jest jednym z kluczowych, niezbędnych elementów do prawidłowego i niezakłóconego działania, w związku z powyższym Kierownictwo Urzędu Gminy celem zagwarantowania poufności, integralności, dostępności i autentyczności informacji związanych z bezpieczeństwem informacji zdecydowało się - w celu sprawnej i skutecznej ochrony tych informacji oraz w konsekwencji – zagwarantowania właściwego świadczenia usług publicznych, ustanowić, wdrożyć oraz utrzymywać System Zarządzania Bezpieczeństwem Informacji (SZBI) właściwy dla zakresu swojej działalności.
5. Ciągłość Działania jest kolejnym krytycznym czynnikiem i warunkiem zapewniającym niezakłócone funkcjonowanie Urzędu, w sytuacji wystąpienia incydentów, jak i w innych sytuacjach poważnych, w tym w sytuacjach kryzysowych. Kierownictwo Urzędu Gminy jest świadome, że wprowadzenie odpowiedniej Polityki Ciągłości Działania oraz Planów Ciągłości Działania opartych na analizie ryzyka oraz analizie ryzyka biznesowego jest kluczowym elementem do zapewnienia ciągłości realizacji zadań i usług społecznych. W związku z powyższym Kierownictwo Urzędu Gminy zdecydowało się na ustanowienie i wdrożenie Systemu Zarządzania Ciągłością Działania (SZCD) zintegrowanego z Systemem Zarządzania Bezpieczeństwem Informacji.

II. Cel i zakres dokumentu

1. Celem wprowadzenia niniejszej Polityki jest zapewnienie spójności kierunków działania i potwierdzenie pełnego wsparcia oraz zaangażowania Kierownictwa Urzędu wraz z pracownikami, w proces planowania, ustanawiania, wdrażania, utrzymywania, monitorowania, przeglądania i doskonalenia SZBI oraz SZCD celem skutecznego zabezpieczenia informacji przetwarzanych w Urzędzie oraz zapewnienia ciągłości działania na wymaganym poziomie.
2. Wszystkie zasady związane z zarządzaniem bezpieczeństwa informacji są ustanawiane, wdrażane oraz doskonalone przy uwzględnieniu charakteru działalności Urzędu oraz wymagań zewnętrznych i wewnętrznych związanych z bezpieczeństwem informacji oraz ciągłością działania.
3. Polityka Bezpieczeństwa Informacji i Ciągłości Działania jest dokumentem stanowiącym fundament działających w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji i Systemu Zarządzania Ciągłością Działania.

4. Polityka określa strukturę zarządzania bezpieczeństwem informacji, w tym zawiera: opis ról i odpowiedzialności, deklarację najwyższego Kierownictwa, zakres SZBI, ogólne wymagania i zasady, zgodnie z którymi są zarządzane, zabezpieczane i eksploatowane aktywa informacyjne, zasady stosowania wyjątków i odstępstw.
5. Polityka określa także najważniejsze zadania oraz zasady zarządzania Ciągłością Działania wraz z zasadami prowadzenia analizy biznesowej.
6. Integralną częścią niniejszej Polityki są Procedury, Instrukcje, Zasady, Standardy oraz Plany (Ciągłości Działania) obowiązujące w Urzędzie Gminy.
7. Niniejsza Polityka, jak i powiązane z nią dokumenty mają zastosowanie i obowiązują:
   a) cały personel Urzędu oraz strony trzecie w zakresie w jakim zostały im one zakomunikowane,
   b) we wszystkich lokalizacjach i komórkach organizacyjnych Urzędu.
   c) Kierownicy jednostek organizacyjnych Gminy Chrzypsko Wielkie, które spełniają przesłanki uznania za podmiot ważny, w szczególności na podstawie art. 5 ust. 2 pkt 8 ustawy o KSC, i realizują zadania publiczne z wykorzystaniem systemów informacyjnych, zapewniają wykonanie obowiązków wynikających z ustawy o KSC w swoich jednostkach. Niniejsza Polityka może być stosowana w tych jednostkach po jej formalnym wprowadzeniu albo w zakresie objętym wspólną obsługą cyberbezpieczeństwa ustanowioną zgodnie z art. 16e-16h ustawy o KSC.
   d) Jeżeli Gmina ustanowi wspólną obsługę obowiązków z zakresu cyberbezpieczeństwa albo zawrze porozumienie w tym zakresie, jednostki obsługiwane współpracują z jednostką wyznaczoną, w szczególności przekazują informacje o incydentach i wykonują decyzje kierownika jednostki wyznaczonej dotyczące SZBI, na zasadach określonych w art. 16f-16h ustawy o KSC.

III. Podstawy dla Systemu Zarządzania Bezpieczeństwem Informacji

1. System Zarządzania Bezpieczeństwem Informacji (SZBI) jest wdrażany, utrzymywany i doskonalony zgodnie z powszechnie obowiązującymi przepisami obowiązującymi Rzeczypospolitej Polskiej oraz w Unii Europejskiej.
2. SZBI spełnia minimalne wymagania dla podmiotu ważnego będącego podmiotem publicznym, określone w art. 8 ust. 3 oraz Załączniku nr 4 do ustawy o KSC. Normy i standardy międzynarodowe, w tym PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005 i PN-EN ISO 22301, są wykorzystywane pomocniczo do projektowania, utrzymywania i doskonalenia zabezpieczeń.
3. W ramach ustawowego minimum SZBI Urzędu obejmuje co najmniej następujące działania i zabezpieczenia:
   a) prowadzenie i aktualizowanie inwentaryzacji produktów ICT, usług ICT i procesów ICT służących do przetwarzania informacji;
   b) kontrolowanie podstawowych wersji używanych produktów ICT i usług ICT oraz - gdy jest to możliwe - kontrolowanie instalacji oprogramowania i usług na urządzeniach, w tym mobilnych;
   c) zapewnienie ochrony informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniem lub zakłóceniem, w tym ochrony fizycznej miejsc przetwarzania, zabezpieczeń programowych i sprzętowych oraz udokumentowania mechanizmów ochrony przy korzystaniu z chmury obliczeniowej lub centrum przetwarzania danych;
   d) dopuszczanie do informacji i systemów informacyjnych wyłącznie osób posiadających odpowiednie uprawnienia oraz stosowanie środków zapobiegających nieautoryzowanemu dostępowi;
   e) stosowanie zasady minimalnych uprawnień niezbędnych do realizacji zadań;

f) bezzwłoczne cofanie uprawnień w razie ustania podstawy dostępu oraz zawieszanie uprawnień w przypadku niewykonywania obowiązków co najmniej przez miesiąc;
g) modyfikowanie zakresu uprawnień odpowiednio do zmian zadań i potrzeb dostępu;
h) ustanowienie zasad bezpiecznej pracy mobilnej i pracy na odległość;
i) kontrolowanie usług poczty elektronicznej z wykorzystaniem wymaganych mechanizmów ochrony przed nadużyciami w komunikacji elektronicznej;
j) wykonywanie kopii zapasowych danych odseparowanych logicznie i fizycznie od danych produkcyjnych;
k) regularne testowanie kompletności kopii zapasowych i możliwości odtworzenia danych;
l) przygotowanie i testowanie procedur działania na wypadek awarii lub incydentu;
m) stosowanie aktualnego oprogramowania antywirusowego lub równoważnych mechanizmów ochronnych;
n) stosowanie zasad cyberhigieny przez pracowników oraz Wójta jako kierownika podmiotu;
o) monitorowanie częstotliwości wydawania nowych wersji, źródeł dystrybucji i cyklu życia produktów ICT;
p) stosowanie stabilnych wersji produktów ICT i usług ICT, co do których nie występują informacje o krytycznych podatnościach, a gdy jest to niemożliwe - stosowanie rozwiązań ograniczających ryzyko do poziomu akceptowalnego;
q) szkolenie osób uczestniczących w przetwarzaniu informacji, obejmujące co najmniej cyberzagrożenia, cyberhigienę, reagowanie na incydenty oraz skutki naruszania zasad bezpieczeństwa;
r) utrzymywanie procedur i zasad działania na wypadek cyberzagrożenia albo incydentu oraz dokumentowanie realizacji działań przewidzianych w SZBI.

4. W SZBI uwzględnia się również systemy informacyjne dostarczane Urzędowi przez inne podmioty publiczne, w zakresie odpowiadającym kompetencjom Urzędu oraz zasadom wynikającym z polityk bezpieczeństwa tych systemów lub z przepisów prawa.

IV. Podstawy dla Systemu Zarządzania Ciągłością Działania

1. System Zarządzania Ciągłością Działania (SZCD) jest wdrażany, utrzymywany i doskonalony zgodnie z powszechnie obowiązującymi przepisami obowiązującymi w Rzeczypospolitej Polskiej oraz w Unii Europejskiej.
2. SZCD opiera się na normach i standardach międzynarodowych, w tym na normie PN-EN ISO/IEC 22301.

V. Deklaracja Najwyższego Kierownictwa

1. Kierownictwo Urzędu Gminy wraz z podległą kadrą kierowniczą jest świadome, że informacja jest jednym z kluczowych zasobów Urzędzie i wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych informacji oraz wyraża gotowość do udzielania wsparcia dla wszelkich rozsądnych przedsięwzięć związanych z ochroną tych informacji.
2. Kierownictwo Urzędu Gminy wraz z podległą kadrą kierowniczą jest świadome, że utrzymywana na wymaganym poziomie ciągłość działania jest kolejnym kluczowym zasobem Urzędu Gminy i wyraża pełne zaangażowanie dla zapewnienia nieprzerwanego funkcjonowania świadczonych usług społecznych oraz wyraża gotowość do udzielania wsparcia dla wszelkich rozsądnych przedsięwzięć związanych z zapewnieniem ciągłości działania.
3. Kierownictwo Urzędu Gminy deklaruje zapewnienie niezbędnych zasobów (sił i środków) do wdrożenia i eksploatacji systemu zarządzania bezpieczeństwem informacji jak i systemu zarządzania ciągłością działania oraz ciągłe doskonalenie wskazanych systemów.

4. Kierownictwo Urzędu Gminy wraz z podległą kadrą kierowniczą deklaruje również pełne zaangażowanie wszystkich pracowników we wdrożenie i utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji i Systemu Zarządzania Ciągłością Działania w oparciu o normy ISO 27001 oraz ISO 22301 oraz w odniesieniu do innych normatywnych aktów prawnych mających zastosowanie do ochrony informacji, ochrony danych osobowych oraz bezpieczeństwa cybernetycznego i jego stałe doskonalenie dla zapewnienia Obywatelom coraz wyższych standardów usług i poczucia bezpieczeństwa, jak i utrzymywania usług krytycznych (priorytetowych) na najwyższym możliwym poziomie.

VI. Opis ról i odpowiedzialności w obszarze SZBI i CD

1. **Kierownictwo Urzędu Gminy Chrzypsko Wielkie wraz z kadrą kierowniczą** odpowiada za ustanowienie, wdrożenie, utrzymywanie oraz doskonalenie niniejszej Polityki Bezpieczeństwa Informacji i Ciągłości Działania oraz określenie ról i przypisanie odpowiedzialności oraz zapewnienie zasobów (sił i środków) niezbędnych do prawidłowego funkcjonowania w pełnym zakresie, wraz z doskonaleniem, Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemu Zarządzania Ciągłością Działania. Osoby odpowiedzialne za pracę poszczególnych komórek organizacyjnych nadzorują zapewnienie bezpieczeństwa informacji i ciągłości działania na wszystkich szczeblach zarządzania i kierowania.
2. Wójt Gminy Chrzypsko Wielkie, jako kierownik podmiotu ważnego będącego podmiotem publicznym, ponosi odpowiedzialność za wykonywanie obowiązków z zakresu cyberbezpieczeństwa również wtedy, gdy obowiązki te powierzono innej osobie za jej zgodą. Wójt podejmuje decyzje dotyczące przygotowania, wdrażania, stosowania, przeglądu i nadzoru SZBI, planuje adekwatne środki finansowe, przydziela zadania z zakresu cyberbezpieczeństwa i nadzoruje ich wykonanie, zapewnia świadomość obowiązków przez personel oraz zgodność działania Urzędu z prawem i regulacjami wewnętrznymi, a także raz w roku kalendarzowym odbywa udokumentowane szkolenie, zgodnie z art. 8c-8e ustawy o KSC.
3. Przed dopuszczeniem osoby do realizacji zadań, o których mowa w art. 8 lub art. 11 ustawy o KSC, Wójt zapewnia spełnienie wymogu z art. 8f tej ustawy: osoba przedstawia informację z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji, chyba że posiada ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej. W razie uzasadnionego podejrzenia skazania osoba jest wzywana do ponownego przedstawienia informacji z KRK. Czynności te podlegają udokumentowaniu.
4. **Osoby odpowiedzialne za pracę poszczególnych komórek organizacyjnych Urzędu, zgodnie z zakresem odpowiedzialności wynikającym z zapisów Regulaminu Organizacyjnego oraz wewnętrznej dokumentacji z zakresu SZBI oraz SZCD,** odpowiadają w szczególności za:
   a) nadzorowanie zapewnienia bezpieczeństwa informacji i ciągłości działania na wszystkich szczeblach zarządzania i kierowania;
   b) stosowanie się do niniejszej Polityki;
   c) określenie i zgłaszanie potrzeby dodatkowych zasobów niezbędnych do realizacji postanowień zawartych w niniejszej Polityce oraz w powiązanych z nią Procedur/ Instrukcji/ Standardów/ innych dokumentów;
   d) zarządzanie ryzykiem bezpieczeństwa dla danego aktywu;
   e) nadzór nad określeniem, wdrożeniem i funkcjonowaniem zabezpieczeń;
   f) zgłaszanie zdarzeń, incydentów w określonym czasie;
   g) współpracę z Pełnomocnikiem ds. Bezpieczeństwa Informacji i Ciągłości Działania, Inspektorem Ochrony Danych Osobowych, Administratorem Systemu Informatycznego, Koordynatorami ds. bezpieczeństwa

fizycznego, środowiskowego i technicznego oraz bezpieczeństwa osobowego oraz pozostałymi pracownikami Urzędu w zakresie zapewnienia bezpieczeństwa aktywów informacyjnych;
h) udział i przyczynianie się do audytów;
i) zarządzanie procesem obsługi incydentów z zakresu bezpieczeństwa informacji;
j) opracowanie i wdrożenie działań minimalizujących skutki wystąpienia incydentu;
k) analizę przyczyny wystąpienia incydentów oraz ich usunięcie.

5. **Pełnomocnik ds. bezpieczeństwa informacji i ciągłości działania** – odpowiada za:
   a) nadzorowanie funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania;
   b) nadzorowanie przestrzegania niniejszej Polityki oraz dokumentów z nią powiązanych;
   c) nadzorowanie wdrożenia, utrzymywania i doskonalenia przyjętych procesów CD;
   d) nadzorowanie opracowania i wdrożenia programów doskonalących funkcjonowanie wdrożonego Systemu CD;
   e) nadzór nad opracowywaniem Planów Ciągłości Działania;
   f) koordynowanie procesu analizy ryzyka dla bezpieczeństwa informacji;
   g) monitorowanie poziomu bezpieczeństwa informacji w Urzędzie;
   h) zbieranie informacji o skuteczności stosowanych zabezpieczeń;
   i) doradzanie i udzielanie wsparcia Kierownictwu Urzędu w zakresie stosowania zasad wynikających z niniejszej Polityki i dokumentów z nią powiązanych;
   j) monitorowanie działań korygujących i doskonalących;
   k) koordynowanie audytów bezpieczeństwa;
   l) nadzorowanie przygotowywania informacji wejściowych do przeglądów zarządzania;
   m) nadzór nad podejmowaniem działań mających na celu utrzymywanie aktualności niniejszej Polityki oraz w razie potrzeby jej aktualizację;
   n) ścisłą współpracą z osobą zatrudnioną na stanowisku ds. informatyki w zakresie zbierania informacji dot. incydentów teleinformatycznych, szacowania ryzyka i przeciwdziałania incydentom teleinformatycznych;
   o) ścisłą współpracę z IOD, Koordynatorami bezpieczeństwa fizycznego, środowiskowego i technicznego oraz osobowego w zakresach określonych procedurami i wymogami w obszarach, za które osoby funkcyjne odpowiadają;
   p) zwoływanie oraz przewodzenie Komitetowi Bezpieczeństwa w zakresie omawiania incydentów, działań korygujących i korekcyjnych, szacowania ryzyka i/lub powstania zmian w kontekście wewnętrznym lub zewnętrznym mogących wpływać na bezpieczeństwo Urzędu;
   q) prowadzenie postępowań wyjaśniających w przypadkach naruszeń bezpieczeństwa związanych z kradzieżą, włamaniem, szpiegostwem przemysłowym, nieautoryzowanym wyciekiem informacji i innymi zdarzeniami mogącymi wpływać w znaczący sposób na bezpieczeństwo Urzędu;
   r) nadzorowanie zbierania i udostępniania materiałów dowodowych dotyczących incydentów bezpieczeństwa

6. **Inspektor Ochrony Danych Osobowych** – odpowiada za:
   a) nadzorowanie zadań z zakresu ochrony danych osobowych;
   b) monitorowanie przestrzegania zapisów Polityki oraz przepisów prawa w zakresie ochrony danych osobowych;
   c) szacowanie ryzyka w zakresie ochrony danych osobowych;
   d) monitorowanie incydentów w zakresie ochrony danych osobowych i przekazywaniu informacji o zaistniałych incydentach do Prezesa UODO;
   e) ścisłą współpracę z Pełnomocnikiem ds. SZBI w zakresie ochrony danych osobowych;

f) uczestniczenie w posiedzeniach Komitetu Bezpieczeństwa.

7. **Koordynator ds. bezpieczeństwa technicznego, środowiskowego i fizycznego -** odpowiada za:
   a) odpowiednie zabezpieczenie serwerowni i centrów przetwarzania danych pod względem technicznym i środowiskowym – w tym za wnioskowanie o wprowadzenie dodatkowych zabezpieczeń;
   b) ścisłą współpracę z Inspektorem ochrony ppoż. oraz Inspektorem BHP;
   c) koordynację działań dezynfekcji, dezynsekcji i deratyzacji;
   d) zapewnienie zasobów w zakresie bezpieczeństwa technicznego urządzeń teleinformatycznych (np. listew antyprzepięciowych, urządzeń UPS, podzespołów chłodzących itp.);
   e) aktualizację niniejszej procedury w koordynacji z Pełnomocnikiem ds. bezpieczeństwa informacji i ciągłości działania w obszarze bezpieczeństwa technicznego i środowiskowego;
   f) nadzór nad procesowaniem wyboru firmy świadczącej usługi ochrony fizycznej dla Urzędu;
   g) wyznaczenie w systemie dyżurowym osób odpowiedzialnych za przyjmowanie zgłoszeń o incydentach w obszarze ochrony fizycznej;
   h) nadzór nad ochroną fizyczną;
   i) wyznaczenie osób do telefonicznego dyżuru 24/7 celem odbierania informacji na temat niepożądanych zdarzeń (incydentów) z zakresu bezpieczeństwa fizycznego,
   j) wyznaczenie stref bezpieczeństwa;
   k) nadzór nad zakupami potrzebnego sprzętu i wyposażenia w obszarze ochrony fizycznej;
   l) systematyczne przeglądy sprzętu i wyposażenia w obszarze ochrony fizycznej;
   m) przygotowanie procedur wydawania kluczy i jej systematyczny przegląd;
   n) nadzór nad systemem kontroli dostępu (SKD), systemem monitoringu przemysłowego (CCTV) oraz systemem sygnalizacji włamania i napadu (SSWiN);
   o) odpowiednie zabezpieczenie serwerowni i centrów przetwarzania danych – w tym za wnioskowanie o wprowadzenie dodatkowych zabezpieczeń;
   p) udział w obradach Komitetu Bezpieczeństwa;
   q) ścisłą współpracę z Pełnomocnikiem ds. BI i CD.

8. **Osoba zatrudniona na stanowisku ds. informatyki /** Administrator Systemów Informatycznych – odpowiada za:
   a) odpowiednie rozłożenie okablowania serwerowni;
   b) odpowiednie usytuowanie urządzeń niepowodujących nadmiernego nagrzewania się itp.;
   c) monitorowanie bezpieczeństwa teleinformatycznego Urzędu;
   d) nadzorowanie bezpieczeństwa fizycznego stref szczególnych dla bezpieczeństwa teleinformatycznego;
   e) nadzorowanie przestrzegania procedur bezpieczeństwa teleinformatycznego;
   f) reagowanie na incydenty teleinformatyczne w tym zgłaszanie właściwym Zespołom Reagowania na Incydenty Bezpieczeństwa, incydentów teleinformatycznych zgodnie z zapisami ustawy o krajowym systemie cyberbezpieczeństwa;
   g) szacowanie ryzyka w zakresie zagrożeń cybernetycznych;
   h) monitorowanie działań korygujących i doskonalących w zakresie bezpieczeństwa teleinformatycznego;
   i) ścisłą współpracę z Pełnomocnikiem ds. BI i CD i zgłaszanie Pełnomocnikowi wszelkich incydentów jako dane wejściowe do przeglądów zarządzania oraz raportowania Kierownictwu Urzędu;

j) udział w obradach Komitetu Bezpieczeństwa;
k) zapewnienie wyznaczenia co najmniej jednej osoby odpowiedzialnej za utrzymywanie kontaktów z innymi podmiotami kluczowymi lub podmiotami ważnymi, zgodnie z art. 9 ust. 3 ustawy o KSC, oraz zapewnienie aktualności danych kontaktowych wykorzystywanych w relacjach z właściwym CSIRT sektorowym;
l) jeżeli osoba zatrudniona na stanowisku ds. informatyki /Administrator Systemów Informatycznych realizuje zadania, o których mowa w art. 8 lub art. 11 ustawy o KSC - spełnienie przed rozpoczęciem tych zadań wymogu określonego w art. 8f ustawy o KSC;

9. **Wewnętrzne struktury cyberbezpieczeństwa** (rola może być delegowana na zewnątrz w ramach outsourcingu) – odpowiadają za:
   a) prowadzenie czynności umożliwiających wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów poprzez ciągły monitoring sieci;
   b) przekazywanie, w niezbędnym zakresie, informacji właściwemu CSIRT sektorowemu oraz innym właściwym podmiotom krajowego systemu cyberbezpieczeństwa, zgodnie z właściwością i obowiązującym kanałem komunikacji;
   c) klasyfikowanie incydentów;
   d) zgłaszanie incydentów poważnych niezwłocznie, nie później niż w ciągu 72 godzin od momentu wykrycia, do właściwego CSIRT sektorowego za pomocą właściwego systemu teleinformatycznego; zgodnie z art. 12c ustawy o KSC Urząd jako podmiot ważny będący podmiotem publicznym nie przekazuje odrębnego wczesnego ostrzeżenia, sprawozdania okresowego, sprawozdania z postępu obsługi incydentu ani sprawozdania końcowego;
   e) obsługę incydentów we współpracy z właściwym CSIRT sektorowym oraz, gdy jest to wymagane, z CSIRT NASK, CSIRT GOV lub CSIRT MON;
   f) wykrywanie, analizę i usuwanie podatności;
   g) przekazywanie Kierownictwu Urzędu, informacji dotyczących incydentu mającego wpływ na ciągłość świadczenia usługi;
   h) ścisłą współpracę z Pełnomocnikiem ds. Bezpieczeństwa Informacji i Ciągłości Działania oraz z Osobą zatrudnioną na stanowisku ds. informatyki/Administratorem Systemu Informatycznego.

10. **Koordynator ds. bezpieczeństwa osobowego, budowy świadomości i szkoleń/ Osoba zatrudniona na stanowisku odpowiedzialnym za kadry** – odpowiada za:
   a) sprawowanie nadzoru nad bezpieczeństwem osobowym w Urzędzie poprzez wprowadzanie procedur, instrukcji i zapisów, jak i wprowadzanie aktualizacji do istniejących dokumentów we wszystkich etapach zatrudnienia pracownika;
   b) ścisłą współpracę z Pełnomocnikiem ds. BI i CD i zgłaszanie Pełnomocnikowi wszelkich incydentów jako dane wejściowe do przeglądów zarządzania oraz raportowania kierownictwu Urzędu.
   c) realizację rozmów z zatrudnianymi pracownikami w zakresie bezpieczeństwa osobowego (prawa, obowiązki i sankcje związane z bezpieczeństwem informacji);
   d) sporządzanie analiz w zakresie potencjalnych zagrożeń ze strony pracowników w obszarze bezpieczeństwa informacji i korupcji;
   e) przygotowywanie materiałów dowodowych w przypadku incydentu związanego z nieautoryzowanym wyciekiem informacji lub podejrzeniem korupcji;
   f) opracowanie programu budowy świadomości;
   g) promowanie kultury jakości, etyki zawodowej, ciągłości działania i bezpieczeństwa informacji,

h) przekazanie programu budowy świadomości do akceptacji Kierownika Urzędu;
i) dystrybucję programu budowy świadomości w organizacji po akceptacji;
j) nadzór nad realizacją programu budowy świadomości;
k) nadzór nad szkoleniami;
l) nadzór nad pozostałymi działaniami uświadamiającymi;
m) monitorowanie wskaźników efektywności programu budowy świadomości;
n) jeżeli jest taka potrzeba – wprowadzenie zmian w programie budowy świadomości;
o) przechowywanie programów budowy świadomości, programów szkoleń, materiałów merytorycznych, dydaktycznych;
p) udział w obradach Komitetu Bezpieczeństwa.

11. **Komitet Bezpieczeństwa:**
1) odpowiada za:
a) wsparcie Kierownictwa Urzędu w zakresie BI oraz CD, w celu wypracowania przez Kierownictwo Urzędu Gminy właściwych decyzji w odniesieniu do Bezpieczeństwa Informacji oraz Ciągłości Działania;
b) analizę zaistniałych poważnych i krytycznych incydentów bezpieczeństwa i podejmowanie decyzji w zakresie krytyczności i wpływu incydentu na funkcjonowanie Urzędu, jak i przygotowywanie raportu dla Kierownictwa Urzędu w przedmiotowej sprawie – po zwołaniu przez Pełnomocnika ds. BI i CD;
c) opracowanie i wdrożenie sankcji za naruszenie zasad bezpieczeństwa;
d) analizę poważnych niezgodności mogących skutkować poważnymi konsekwencjami dla Urzędu i przygotowywanie rekomendacji w sprawie ewentualnych działań korygujących i korekcyjnych – po zwołaniu przez Pełnomocnika ds. BI i CD lub przez Kierownika Urzędu;
e) przeprowadzenie procedury zarządzania ryzykiem co najmniej raz 12 miesięcy lub każdorazowo po zmianie kontekstu wewnętrznego i/lub zewnętrznego;
f) przegląd dokumentacji bezpieczeństwa zgodnie z zapisami lub w przypadku zmiany kontekstu wewnętrznego i/lub zewnętrznego;
g) udział w audytach wewnętrznych.
2) **Komitetowi bezpieczeństwa przewodzi Pełnomocnik ds. Bezpieczeństwa Informacji i Ciągłości Działania.**
3) Komitet zwoływany jest przez Pełnomocnika ds. BI i CD lub przez Kierownika Urzędu samodzielnie lub na wniosek innego członka Komitetu oraz raz na 12 miesięcy na dwa tygodnie przez Przeglądem Zarządzania celem przygotowania informacji oraz szacowania ryzyka na Przegląd Zarządzania.
4) W skład Komitetu w ramach członkostwa stałego wchodzą:
a) Pełnomocnik ds. BI i CD;
b) Inspektor Ochrony Danych Osobowych;
c) Koordynator ds. bezpieczeństwa osobowego, budowy świadomości i szkoleń/ Osoba zatrudniona na stanowisku odpowiedzialnym za kadry;
d) Koordynator ds. bezpieczeństwa technicznego, środowiskowego i fizycznego;
e) Osoba zatrudniona na stanowisku ds. informatyki / Administrator Systemów Informatycznych;
f) Inspektor ochrony PPOŻ;
g) Inspektor BHP;
h) Specjalista ds. obronności;

12. **Wewnętrzna komórka audytu** – odpowiada za:
i) przygotowanie planu audytu;
j) przekazanie planu audytu do zatwierdzenia;

k) powiadomienie osób odpowiedzialnych za pracę poszczególnych komórek organizacyjnych o terminie audytu;
l) przeprowadzenie spotkania otwierającego;
m) w koordynacji z Pełnomocnikiem ds. BI i CD, wyznaczenie Audytorów wewnętrznych oraz inne osoby funkcyjne (ekspert, przewodnik);
n) przeprowadzenie audytu;
o) uzgodnienie z komórkami poszczególnych komórek organizacyjnych stwierdzonych niezgodności;
p) przygotowanie raportu z audytu;
q) zapoznanie z raportem Kierownictwa Urzędu.

13. **Pracownicy i Współpracownicy Urzędu** - odpowiadają za zapewnienie bezpieczeństwa przetwarzanym informacjom, stosowanie się do postanowień zawartych w niniejszej Polityce oraz przestrzeganie powiązanych z nią Procedur/Instrukcji/standardów/innych dokumentów.
14. **Strony trzecie** - odpowiadają za zapewnienie bezpieczeństwa przetwarzanym informacjom, stosowanie się do postanowień zawartych w niniejszej Polityce oraz przestrzeganie powiązanych z nią Procedur/Instrukcji/Standardów/innych dokumentów (w zakresie w jakim wskazane dokumenty zostały im zakomunikowane i zostali zobowiązani do ich stosowania).

VII. Cel i zakres Systemu Zarządzania Bezpieczeństwem Informacji

1. Podstawowym celem wdrożenia, utrzymywania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemu Zarządzania Ciągłością Działania w Urzędzie Gminy jest zapewnienie odpowiedniego, adekwatnego poziomu ochrony przetwarzanych informacji, zarówno tych przetwarzanych w formie elektronicznej, jak i papierowej oraz werbalnej, a także zapewnienie braku zakłóceń w procesie udzielania świadczeń publicznych w Urzędzie poprzez wprowadzenie odpowiednich i adekwatnych do zagrożeń Planów Ciągłości Działania.
2. Celem wdrożenia, utrzymywania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji jest osiągnięcie poziomu organizacyjnego i technicznego, który:
   a) będzie zapewniał odpowiednią ochronę informacji (zapewni zachowanie poufności, integralności i dostępności oraz autentyczności informacji (niezależnie od ich formy)) przetwarzanych w Urzędzie oraz zapewni ciągłość procesu ich przetwarzania,
   b) zminimalizuje ryzyko występowania zagrożeń dla bezpieczeństwa informacji,
   c) zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa informacji (np. podczas incydentu),
   d) zapewni odpowiedni poziom obsługi incydentów oraz ograniczy liczbę incydentów występujących w przyszłości.
3. Powyżej wskazane cele są osiągane poprzez:
   a) wyznaczenie celów, kierunków rozwoju i zasad działania dla ustanowienia, wdrożenia i utrzymywania SZBI;
   b) wyznaczenie ról i przypisanie odpowiedzialności oraz przyznanie kompetencji i zapewnienie odpowiednich zasobów (sił i środków) celem utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji;
   c) udzielenie pełnego wsparcia kierownictwu Urzędu wraz z kadrą kierowniczą dla osób odpowiedzialnych za utrzymanie, doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji;
   d) zapewnienie, że bezpieczeństwo informacji stanowi nieodłączną część zarządzania Urzędem Gminy;
   e) opracowywanie Procedur, Instrukcji, standardów oraz pozostałych dokumentów uszczegółowiających zasady dotyczące bezpieczeństwa informacji;

f) prowadzenie systematycznych przeglądów Polityki oraz dokumentów z nią powiązanych oraz ich aktualizację wskazanych dokumentów, tam, gdzie jest to wymagane;
g) zobowiązanie pracowników Urzędzie oraz tam, gdzie jest to właściwe zobowiązanie stron trzecich do stosowania się do przyjętych w Urzędzie, Polityk, Procedur, Instrukcji i standardów określających sposób zabezpieczania informacji;
h) proaktywne podejście do zarządzania ryzykiem, w tym regularne prowadzenie analizy (szacowania) ryzyka oraz opracowywanie planów postępowania z ryzykiem, wdrażanie zabezpieczeń w oparciu o wyniki analizy ryzyka;
i) zarządzanie incydentami oraz wyciąganie wniosków z incydentów, które miały miejsce w Urzędu;
j) prowadzenie weryfikacji i oceny dostawców usług krytycznych pod kątem bezpieczeństwa Urzędu;
k) ciągłe doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji;
l) prowadzenia działań uświadamiających pracowników Urzędzie, w zakresie ich roli w prawidłowe działanie SZBI, w zakresie zapewnienia bezpieczeństwa informacji.

VIII. Cel i zakres Systemu Zarządzania Ciągłością Działania

1. Podstawowym celem wdrożenia i utrzymywania Zarządzania Ciągłością Działania w Urzędzie Gminy jest zapewnienie braku zakłóceń w procesie świadczenia usług publicznych oraz zapewnienie, że w przypadku wystąpienia sytuacji kryzysowej zostaną podjęte zaplanowane działania, tak aby umożliwić normalne działanie Urzędu.
2. Powyżej wskazane cele są osiągane poprzez:
   a) wyznaczenie celów, kierunków rozwoju i zasad działania dla ustanowienia, wdrożenia i utrzymywania Zarządzania Ciągłością Działania;
   b) zapewnienie zgodności podejmowanych działań zgodnie z powszechnie obowiązującym prawem,
   c) wyznaczenie ról i przypisanie odpowiedzialności oraz przyznanie kompetencji w zakresie utrzymania zarządzania ciągłością działania,
   d) wsparcie Kierownictwa Urzędu dla osób odpowiedzialnych za utrzymanie, doskonalenie zarządzania ciągłością działania,
   e) minimalizację prawdopodobieństwa wystąpienia awarii dla krytycznych zasobów i usług świadczonych przez Urząd,
   f) systematyczne prowadzenie przeglądów i aktualizację procedur zarządzania ciągłością działania,
   g) budowę świadomości pracowników i współpracowników Urzędzie z zakresu zarządzania ciągłością działania i ich roli w jego budowie,
   h) zapewnienie zasobów niezbędnych do prawidłowego i skutecznego funkcjonowania oraz doskonalenia zarządzania ciągłością działania,
   i) proaktywne podejście do zarządzania ryzykiem, w tym regularne prowadzenie analizy ryzyka oraz opracowywanie planów postępowania z ryzykiem, wdrażanie zabezpieczeń w oparciu o wyniki analizy ryzyka,
   j) prowadzenia analizy ciągłości działania,
   k) proaktywne zarządzanie incydentami,
   l) opracowywanie planów ciągłości działania oraz ich regularne testowanie.

IX. Podstawowe metody zarządzania bezpieczeństwem informacji

1. Najważniejsze role i odpowiedzialności związane z zarządzeniem bezpieczeństwem informacji w Urzędzie zostały opisane w niniejszej Polityce oraz uszczegółowione w dokumentach ją wspierających (tam, gdzie jest to zasadne).

2. Proces zarządzania ryzykiem jest realizowany zgodnie z Procedurą zarządzania ryzykiem.
3. Wymagania bezpieczeństwa, środki zabezpieczeń są dobierane w oparciu o wyniki szacowania ryzyka.
4. Równie ważne jest monitorowanie i ocena skuteczności wdrożonych środków zabezpieczeń informacji – wskazane jest realizowane m.in. poprzez monitorowanie skuteczności wdrożonych zabezpieczeń, zarządzanie podatnościami oraz prowadzenie audytów wewnętrznych oraz monitorowanie mierników bezpieczeństwa. W tym celu w Urzędzie Gminy Chrzypsko Wielkie stosuje się narzędzia monitorujące sieć komputerową, w tym stacje robocze.
5. Kolejnym istotnym elementem jest zapewnienie dostępu do wiedzy personelowi Urzędu, tak aby byli świadomi jaka jest ich rola i jakie są ich obowiązki oraz jaki mają wpływ na działanie SZBI, jest to zapewniane poprzez prowadzenie cyklicznych działań uświadamiających dla personelu Urzędu.
6. Istotnym elementem jest również zachowanie czujności przez personel i niezwłoczne zgłaszanie wszelkich zaobserwowanych zdarzeń związanych z bezpieczeństwem oraz słabości/niezgodności. Pozwala to na wczesne reagowania na występujące incydenty oraz proaktywne podejście do zarządzania bezpieczeństwem. Zgłoszenia oraz zarządzanie incydentami jest realizowane zgodnie z procedurą Zarządzania incydentami.
7. Kolejnym istotnym elementem jest konieczność ciągłego doskonalenia wdrożonego i utrzymywanego systemu zarządzania, które jest realizowane przez Urząd, m.in. poprzez zachęcanie pracowników do zgłaszania działań doskonalących, monitorowanie procesów oraz wdrożonych zabezpieczeń, prowadzenie audytów wewnętrznych, monitorowanie celów i mierników bezpieczeństwa informacji, prowadzenie systematycznych analiz zagrożeń oraz przeglądów zarządzania, a także sprawowanie nadzoru nad dostawcami i zarządzanie podatnościami.

X. Plany ciągłości działania

1. Plany ciągłości działania są opracowywane dla wszystkich aktywów, bez których, nie jest możliwe realizowanie usług publicznych przez Urząd Gminy na zdefiniowanym poziomie działania.
2. Właściciele kluczowych aktywów zobowiązani są do opracowania planów ciągłości działania i przekazania ich do uzgodnienia Pełnomocnikowi ds. BI i CD, który weryfikuje je i przedkłada do zatwierdzenia Kierownictwu Urzędu.
3. Plany ciągłości działania podlegają przeglądowi przez Komitet Bezpieczeństwa obradujący pod przewodnictwem Pełnomocnika ds. Bezpieczeństwa Informacji i Ciągłości Działania z wiodącą rolą w tym obszarze Pełnomocnika ds. BI i CD, nie rzadziej niż co 12 miesięcy lub w przypadku wystąpienia istotnych zmian wpływających na sposób działania Urzędu.
4. Plany ciągłości działania są testowane, a wyniki tych testów są dokumentowane przez Pełnomocnika ds. BI i CD.

XI. Plany Awaryjne Systemu teleinformatycznego

1. **Osoba zatrudniona na stanowisku ds. informatyki /** Administrator Systemów Informatycznych:
   a) zapewnia ustanowienie procedur oceny i odzyskiwania systemu po jego awarii;
   b) zapewnia kluczowe informacje potrzebne do odzyskiwania systemu, w tym role i obowiązki, informacje o zasobach, procedury oceny sytuacji, szczegółowe procedury odzyskiwania i testowanie systemu;
   c) opracowuje procedury planu awaryjnego systemu informatycznego, które mają na celu odzyskanie systemu niezależnie od lokalizacji;

d) na podstawie wyników analizy BIA i oceny ryzyka naruszenia Ciągłości działania Systemu informatycznego podejmuje działania korygujące, naprawcze i doskonalące;
e) opracowuje harmonogram testowania planów awaryjnych oraz przeprowadza ich testowanie, dokumentując wyniki.

XII. Postanowienia ogólne dotyczące Analizy Ciągłości Działania

1. Analiza wpływu zdarzenia na działalność strategiczną (Business Impact Analysis – BIA) jest postępowaniem w trakcie, którego identyfikowane są krytyczne procesy i zasoby niezbędne do utrzymania bądź wznowienia procesów w Urzędzie Gminy. Podczas prowadzenia BIA są również określane skutki przerwania tych procesów.
2. Celem prowadzenia analizy BIA jest identyfikacja zagrożeń (ryzyk) wraz z zidentyfikowaniem sposobów przeciwdziałania potencjalnym zagrożeniom.
3. W ramach Analizy BIA określane są również kluczowe wskaźniki dotyczące docelowego czasu odtworzenia procesu i zasobów (tzw. Recovery Time Objective - RTO) i (tzw. Recovery Point Objective - RPO) oraz budowana jest Minimalna Akceptowalna Konfiguracja (MAK) dla procesów.

XIII. Zasady prowadzenia analizy BIA

1. Analiza BIA (wpływu na działalność) prowadzona jest dla procesów krytycznych lub zasobów krytycznych zidentyfikowanych w Urzędzie.
2. Dla każdego z procesów krytycznych lub zasobów krytycznych analizowane są skutki niedostępności w czasie i w wymiarze:
   a) Strat finansowych
   b) Strat wizerunkowych
3. Do określenia strat wymienionych w ust. 2 stosowana jest skala wskazana w poniższej tabeli:

Poziom strat	Opis
K- krytyczne	Straty finansowe lub wizerunkowe mogą zagrozić zdolności Urzędu do kontynuowania działalności.
P- poważne	Straty finansowe lub wizerunkowe będą odczuwalne dla Urzędu, ale nie zagrożą zdolności Urzędu do kontynuacji działalności.
A – akceptowalne	Straty finansowe lub wizerunkowe nie będą odczuwalne dla Urzędu.

4. Ponadto w Analizie BIA określane są czasy tj.:
   a) MTPD (Maximum Tolerable Time of Disruption) – maksymalny akceptowalny czas przestoju,
   b) RTO (Recovery Time Objective) – planowany czas odtwarzania,
   c) RPO (Recovery Point Objective) – planowany punkt odtwarzania w czasie.
5. Do analizy BIA wykorzystywana jest macierz, w której w straty dla poszczególnych czasów określane są zgodnie z skalą opisaną w ust. 3 nini:

Proces lub zasób krytyczny: **nazwa procesu krytycznego lub zasobu**

Czas niedostępności	0,2 g	0, 5g	1 g	4 g	8 g	24 g	48 g	1 t	2 t	1 m	3 m	6 m
Straty finansowe												

Straty wizerunkowe												

Legenda: g – godzin; t – tygodni; m – miesięcy

OPIS SYTUACJI	Brak dostępu do			
ROLE I ODPOWIEDZIALNOŚCI				
URUCHOMIENIE PLANU	Decyzję o uruchomieniu planu podejmuje			
KOMUNIKACJA				
PLAN DZIAŁAŃ	**Lp.**	**Działanie**	**Kto wykonuje**	**Uwagi**
	1.			
	2.			
	3.			

Wyznaczone parametry												
MTPD												
RTO												
RPO												

6. Następnie przeprowadzana jest ocena, czy czasy RTO i RPO są akceptowalne, czy nie są akceptowalne.
7. Jeżeli nie są akceptowalne, to konieczne jest zaplanowanie działań związanych z tym ryzykiem (w ramach planu postępowania z ryzykiem).
8. Kolejnym krokiem jest określanie rezydualnych czasów RTO i RPO oraz przeprowadzanie ponownej oceny akceptowalności czasów RTO i RPO.
9. Ostatnim krokiem jest opracowanie, udokumentowanego raportu z analizy BIA.

XIV. Przykładowy Plan Ciągłości Działania

1. Plan ciągłości działania
2. Plan odtworzenia działalności

	Lp.	**Działanie**	**Wykonuje**	**Uwagi**
PLAN ODTWARZANIA	**1.**			
	2.			
	3.			

3. Proces wycofania planu

	Lp.	**Działanie**	**Wykonuje**	**Uwagi**
PROCES WYCOFANIA PLANU	**1.**			
	2.			

	3.			

4. Plan przygotowania

SPIS NIEZBĘDNYCH ZASOBÓW	Lp.	Spis zasobów	Wykonuje	Uwagi
	1.			
	2.			
PLAN SZKOLENIA	Lp.	Działanie	Wykonuje	Uwagi
	1.		.....	
	2.		.....	

XV. Wyjątki i Odstępstwa

1. W sytuacjach, w których spełnienie wymagań niniejszej Polityki lub związanych z nią Regulacji Wewnętrznych dotyczących bezpieczeństwa informacji i/lub ciągłości działania nie jest możliwe lub nie jest racjonalne, istnieje możliwość odstąpienia od spełniania tych wymagań, o ile taka sytuacja nie pozostaje w sprzeczności z wymogami prawa.
2. Wnioski o odstępstwo/wyjątek zawierający uzasadnienie potrzeby zastosowania odstępstwa/wyjątku od stosowania niniejszej Polityki lub dokumentów z nią powiązanych zgłaszane są do Pełnomocnika ds. BI i CD, który rozpatruje otrzymane zgłoszenie, z zastrzeżeniem p. 3) poniżej.
3. W przypadku gdy:
   a) wniosek o odstępstwo zgłaszany jest przez IOD (w przypadku odstępstw dotyczących ochrony danych osobowych) lub
   b) w ocenie IOD nie powinno mieć miejsce odstępstwo/wyjątek od niniejszej Polityki,

   wniosek kierowany jest bezpośrednio do Kierownika Urzędu (Wójta), który podejmuje ostateczną decyzję o sposobie jego rozpatrzenia.
4. Wszelkie odstępstwa i wyjątki rejestrowane są przez Pełnomocnika ds. BI i CD oraz są przez niego monitorowane.
5. Pełnomocnik ds. BI i CD systematycznie (co najmniej raz na kwartał) analizuje ryzyko związane z odstępstwami, ocenia, czy odstępstwo może zostać wyeliminowane oraz przynajmniej raz w roku przedstawia wnioski w tym zakresie Kierownictwu Urzędu, w przypadku możliwości wyeliminowania odstępstwa, Pełnomocnik niezwłocznie informuje o tym Kierownika Urzędu.
6. W przypadku odstępstw i wyjątków dotyczących ochrony danych osobowych Pełnomocnik ds. BI i CD współpracuje i koordynuje wszelkie wyjątki i odstępstwa z IOD.

XVI. Brak stosowania zasad – odpowiedzialność

1. Pracownicy Urzędu (pracownicy, praktykanci, stażyści i współpracownicy na podstawie umów cywilnych) zobowiązani są do zapoznania się z niniejszą Polityką oraz do stosowania się do postanowień w niej zawartych i dokumentach z nią powiązanych.
2. Brak stosowania się do obowiązujących w Urzędzie Gminy dokumentów z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania może być podstawą do nałożenia kar porządkowych na pracowników oraz

wypowiedzenia lub rozwiązania umowy przez Kierownika Urzędu z osobą łamiącą zasady bezpieczeństwa obowiązujące w Urzędzie.

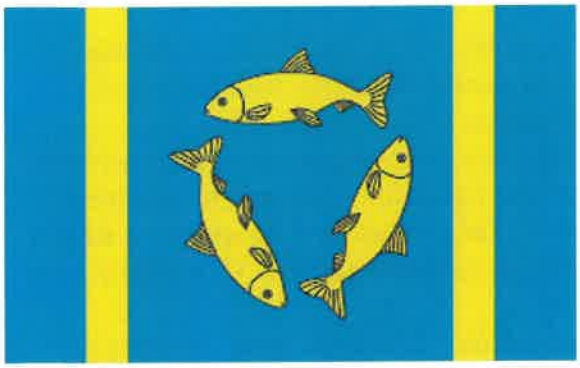
XVII. Postanowienia końcowe

1. Niniejsza Polityka jest dostępna dla wszystkich stron zainteresowanych w szczególności dla wszystkich pracowników Urzędzie.
2. Niniejsza Polityka jest dostępna dla stron zainteresowanych u Pełnomocnika ds. BI i CD, a w przypadku delegowania uprawnień na zewnątrz, u osoby wyznaczonej przez Wójta.

XVIII. Przeglądy oraz aktualizacje Polityki

1. Przegląd SZBI i niniejszej Polityki jest dokonywany co najmniej raz w roku przez Komitet Bezpieczeństwa pod przewodnictwem Pełnomocnika ds. BI i CD.
2. W przypadku zmiany przepisów lub istotnej zmiany kontekstu działania Urzędu, jak i kontekstu zewnętrznego wpływającego pośrednio i bezpośrednio na funkcjonowanie Urzędu, przegląd niniejszej Polityki jest dokonywany niezwłocznie oraz jeżeli istnieje taka potrzeba dokonywana jest jej aktualizacja. Zgodnie z Załącznikiem nr 4 do ustawy o KSC, przegląd SZBI jest dokonywany bezzwłocznie także w przypadku wydania przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa rekomendacji dotyczącej systemów, produktów lub usług ICT Urzędu oraz w przypadku wystąpienia okoliczności mogących wpłynąć na ryzyko wystąpienia incydentu poważnego; realizacja działań wynikających z SZBI jest dokumentowana.
3. Za aktualizację Polityki odpowiada Pełnomocnik ds. BI i CD, który w celu aktualizacji Polityki zwołuje Komitet bezpieczeństwa.
4. Każda zmiana Polityki musi zostać udokumentowana.
5. W przypadku niewielkich lub kosmetycznych zmian, Pełnomocnik ds. BI i CD nie musi zwoływać obrad Komitetu bezpieczeństwa i przeglądu wraz ze zmianami może dokonać sam lub w pomniejszonym gronie funkcjonalnym zgodnie z obszarami, w których zmiany będą wymagane.

Wójt
mgr inż. Edmund Ziółek



DOKUMENT SYSTEMU ZARZĄDZANIA

BEZPIECZEŃSTWEM INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

Procedura zarządzania ryzykiem

Nazwa dokumentu	**Procedura zarządzania ryzykiem**
Autor dokumentu	Joanna Mrowicka
Sprawdzająca dokument	Aneta Skrzypczak-Kurzawa
Wersja dokumentu	0.2
Zatwierdzający dokument	Wójt Gminy
Data zatwierdzenia dokumentu	15 września 2026r.

I. Cel i zakres dokumentu

1. Celem niniejszej procedury jest określenie kompleksowego podejścia do procesu zarządzania ryzykiem w **Urzędzie Gminy Chrzypsko Wielkie,** w dalszej części zwanym również „Urzędem Gminy" lub „Urzędem".
2. **Procedura opisuje zasady zarządzania ryzykiem związanym z bezpieczeństwem informacji, cyberbezpieczeństwem i ciągłością działania oraz stanowi element SZBI spełniającego wymagania art. 8 ust. 3 i Załącznika nr 4 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20, 252, 815, z późn. zm.).**
3. Dokument obowiązuje wszystkich pracowników Urzędzie oraz obowiązuje we wszystkich lokalizacjach Urzędu.
4. Kierownicy jednostek organizacyjnych Gminy, które spełniają przesłanki uznania za podmiot ważny, w szczególności na podstawie art. 5 ust. 2 pkt 8 ustawy o KSC, i realizują zadania publiczne z wykorzystaniem systemów informacyjnych, zapewniają prowadzenie zarządzania ryzykiem we własnym SZBI albo przekazują wymagane dane do wspólnego procesu zarządzania ryzykiem, jeżeli jednostka jest objęta wspólną obsługą cyberbezpieczeństwa na podstawie art. 16e-16h ustawy o KSC.
5. Procedura jest podstawowym dokumentem metodycznym zarządzania ryzykiem w SZBI i CD. Normy PN-ISO/IEC 27005 oraz inne normy stosuje się pomocniczo; procedura uzupełnia również ocenę ryzyka i analizę skutków prowadzoną na potrzeby ochrony danych osobowych (RODO).

II. Wytyczne dodatkowe

Wójt - na bazie osobnych zapisów wewnętrznych powoła stałe ciało doradcze – Komitet Bezpieczeństwa celem wsparcia procesu zarządzania ryzykiem i wypracowania danych wyjściowych dla ryzyk występujących lub mogących wystąpić w Urzędzie w związku z kontekstem wewnętrznym i zewnętrznym.

III. Role i odpowiedzialności:

1. **Rolą Wójta**, jako kierownika podmiotu ważnego będącego podmiotem publicznym, jest:
   a) podejmowanie decyzji w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru SZBI, w tym ram zarządzania ryzykiem, przy zachowaniu odpowiedzialności wynikającej z art. 8c i 8d ustawy o KSC;
   b) zatwierdzanie kryteriów akceptacji ryzyka oraz podejmowanie decyzji o akceptacji ryzyk wysokich i innych ryzyk wymagających decyzji kierownika;
   c) zapewnienie właścicielom ryzyka zasobów organizacyjnych, technicznych i finansowych niezbędnych do postępowania z ryzykiem;
   d) zapewnienie dokumentowania procesu oraz nadzoru nad realizacją planów postępowania z ryzykiem.
2. Rolą **Pełnomocnika ds. Bezpieczeństwa Informacji i Ciągłości Działania** jest:
   a) Inicjowanie procesu zarządzania ryzykiem,
   b) Nadzorowanie i koordynowanie procesu zarządzania ryzykiem,
   c) Zbieranie informacji niezbędnych do przeprowadzenie procesu szacowania i oceny ryzyka, w szczególności od właścicieli ryzyka,
   d) Dbałość o zapewnienie spójności wyników szacowania ryzyka.
3. Rolą **Komitetu Bezpieczeństwa** jest:
   a) Ocena zebranych informacji niezbędnych do przeprowadzenia procesu szacowania i oceny ryzyka,
   b) Określenie ryzyk dla Urzędu,
   c) Przeprowadzenie szacowania ryzyka wraz z oceną ryzyka dla Urzędu
4. Rolą **Właściciela ryzyka** jest zarządzanie ryzykiem dla którego pełni rolę właściciela w sposób zapewniający, że ryzyko to pozostaje pod kontrolą.
5. Rolą Pracowników Urzędzie jest:

a) Współpraca ze wszystkimi osobami odpowiedzialnym za proces zarządzania ryzykiem oraz zarządzania ryzykiem, w szczególności w zakresie dostarczania informacji związanych z tymi procesami,
b) Zgłaszanie wszelkich słabości swoim przełożonym w zakresie bezpieczeństwa informacji oraz zapewnienia ciągłości działania Urzędu.

IV. Zarządzanie ryzykiem dla bezpieczeństwa informacji i ciągłości działania

1. **Proces zarządzania ryzykiem jest procesem ciągłym. Szacowanie i ocena ryzyka są wykonywane co najmniej raz w roku oraz bezzwłocznie każdorazowo w przypadku:**
   a) Wprowadzenia nowego procesu do Urzędu istotnego z punktu widzenia zachowania ciągłości działania Urzędu lub zapewnienia bezpieczeństwa przetwarzanym informacjom,
   b) Modyfikacji istniejącego procesu istotnego z punktu widzenia zachowania ciągłości działania lub zapewnienia bezpieczeństwa przetwarzanym informacjom;
   c) Istotnej zmiany w kontekście funkcjonowania Urzędu.
   d) wydania przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa rekomendacji dotyczącej systemów informacyjnych, produktów ICT lub usług ICT wykorzystywanych przez Urząd;
   e) wystąpienia okoliczności, które mogą wpłynąć na ryzyko wystąpienia incydentu poważnego, w tym wykrycia krytycznej podatności, istotnego cyberzagrożenia albo istotnej zmiany technologicznej;
   f) wdrożenia lub istotnej zmiany produktu ICT, usługi ICT, procesu ICT, usługi chmurowej, centrum przetwarzania danych albo sposobu świadczenia usługi przez dostawcę;
   g) wystąpienia incydentu poważnego, powtarzających się incydentów lub wyników testów/audytów wskazujących na nieskuteczność zabezpieczeń.
2. **Proces zarządzania ryzykiem składa się z następujących podprocesów:**
   a) Identyfikacji ryzyka,
   b) Szacowania (analiza) ryzyka,
   c) Oceny ryzyka.
3. **Identyfikacja ryzyka**
   a) Proces identyfikacji ryzyka ma za zadanie dostarczyć informacji w jakich obszarach działań znajdują się ryzyka, mogące wpływać na działalność Urzędu Gminy.
   b) Do identyfikacji ryzyka wykorzystuje się katalog zagrożeń z Załącznika nr 1, informacje o incydentach i zdarzeniach historycznych, ostrzeżenia i rekomendacje właściwych organów i CSIRT, informacje o podatnościach, wyniki testów i audytów, informacje od dostawców oraz dane z monitorowania systemów. Katalog zagrożeń ma charakter pomocniczy i nie ogranicza obowiązku identyfikacji nowych lub specyficznych ryzyk.
   c) Krokiem pierwszym jest identyfikacja ryzyka dla aktywów informacyjnych oraz dla zinwentaryzowanych produktów ICT, usług ICT i procesów ICT, w tym systemów dostarczanych przez inne podmioty publiczne. Analiza obejmuje również zależności od dostawców, usług chmurowych i centrów przetwarzania danych, kopii zapasowych, dostępu uprzywilejowanego, pracy zdalnej i mobilnej oraz cyklu życia wykorzystywanych technologii.
   d) Identyfikowane ryzyko może mieć negatywny wpływ na Urząd Gminy i wtedy jest nazywane zagrożeniem lub pozytywny wpływ i wtedy nazywane jest szansą. Zidentyfikowane ryzyko opisywane jest w modelu trzy elementowym: przyczyna – ryzyko - skutek.

e) Krokiem drugim jest określenie aktualnie wdrożonych zabezpieczeń oraz ocena ich skuteczności, w tym zabezpieczeń wymaganych w Załączniku nr 4 do ustawy o KSC: kontroli dostępu i minimalnych uprawnień, ochrony fizycznej, ochrony antymalware, kopii zapasowych i testów odtworzeniowych, zarządzania wersjami i podatnościami, zasad cyberhigieny, szkoleń oraz procedur awaryjnych i incydentowych.

4. **Szacowanie (analiza) ryzyka**
   a) Kierownicy poszczególnych komórek organizacyjnych lub wskazani przez nich Pracownicy wskazują zagrożenia, które mogą się zmaterializować w danym procesie w komórce organizacyjnej.
   b) Komitet Bezpieczeństwa określa współczynnik prawdopodobieństwa materializacji zagrożenia oraz określa jego potencjalne skutki materializacji.
   c) Ocenę prawdopodobieństwa wystąpienia zagrożenia dla każdego z obszarów przedstawia się w sposób ogólny zgodnie ze skalą przedstawioną w tabeli poniżej:

Poziom	Wartość	Opis
5 (Bardzo wysokie)	0,85	Jesteśmy absolutnie przekonani, że jeżeli nic nie zrobimy to tak się stanie. Istnieją racjonalne przesłanki by ocenić, że zagrożenie raczej się zmaterializuje. Zagrożenie jest realne. Prawdopodobieństwo: 85-100%
4 (Wysokie)	0,65	Jesteśmy przekonani, że jeżeli nic nie zrobimy to tak się stanie. Mieliśmy już z tym zagrożeniem problemy (występowało w przeszłości), nie zabezpieczyliśmy się przed tym zagrożeniem, stanowi ono dla nas ważny problem. Wysoce prawdopodobne że zagrożenie wystąpi. Prawdopodobieństwo: 65-84%
3 (Średnie)	0,50	Wystąpienie zagrożenia jest realne. Materializacja zagrożenia oceniamy na okolice 50% Materializowało się sporadycznie w przeszłości w ciągu ostatnich 2 - 3 lat Prawdopodobieństwo: 36-64%
2 (Niskie)	0,35	Zagrożenie materializowało się sporadycznie w przeciągu ostatnich 5 lat. Zagrożenie jest niskie ale ciągle występuje. Prawdopodobieństwo: 16 – 35%
1 (Bardzo niskie)	0,15	Bardzo małe prawdopodobieństwo że zagrożenie wystąpi nie mniej jednak jest realne. Prawdopodobieństwo: 0 – 15%

Ocenę skutków materializacji zagrożenia przedstawia się w pięciostopniowej skali, zgodnie z poniższą tabelą:

Poziom	**Wartość**	**Opis**
5 (Bardzo wysokie)	10	Katastrofalne skutki finansowe, konsekwencje prawne, przerwanie procesów biznesowych oraz ciągłości działania i usług wpływające na Klientów Urzędzie i tym samym na wizerunek jak i funkcjonowanie Gminy.

		Praktycznie brak możliwości zachowania pełnej ciągłości działania
4 (Wysokie)	8	Poważne skutki finansowe, konsekwencje prawne, przerwanie procesów biznesowych wpływające na Klientów Urzędzie i tym samym na wizerunek Gminy. Poważne problemy z zachowaniem ciągłości działania i usług.
3 (Średnie)	5	Przeciętne skutki finansowe, konsekwencje prawne, przerwanie procesów biznesowych wpływające na Klientów Urzędzie i tym samym na wizerunek Gminy. Niewielkie trudności w zachowaniu ciągłości działania.
2 (Średnie)	2	Małe skutki finansowe (kilka-kilkanaście tysięcy zł, zakłócenia procesów biznesowych, które nie wpływają na Klientów Urzędzie. Ciągłość działania zachowana.
1 (Niskie)	1	Drobne wewnętrzne zakłócenie procesu/działania Urzędu - brak konsekwencji finansowych / prawnych. Ciągłość działania zachowana.

5. **Ocena ryzyka**
   a) Ewaluacja oceny ryzyka jest przeprowadzana przez **Komitet Bezpieczeństwa**, której przewodzi Pełnomocnik ds. Bezpieczeństwa Informacji i Ciągłości Działania na podstawie informacji otrzymanych od osób odpowiedzialnych za pracę poszczególnych komórek organizacyjnych i na bazie wcześniej przeprowadzonego szacowania.
   b) Ocenę ryzyka przedstawia się w sposób ogólny za pomocą poniższego wzoru:

R=P x S
R-Ryzyko
S-Skutek materializacji zagrożenia
P-Prawdopodobieństwo materializacji zagrożenia

Wyznaczony podczas analizy poziom ryzyka jest porównywany z określonym progiem akceptowalności, w celu określenia sposobu postępowania z ryzykiem

Poziom ryzyka - R	Skutki – S (1-5)				
Prawdopodobieństwo - P (1-5)	1 (1)	2 (2)	3 (5)	4 (8)	5 (10)
1 (0,15)	0,15	0,3	0,75	1,2	1,5
2 (0,35)	0,35	0,7	1,75	2,8	3,5
3 (0,50)	0,5	1,0	2,5	4	5
4 (0,65)	0.65	1,3	3,25	5,2	6,5
5 (0,85)	0,85	1,7	4,25	5,2	8,5

Macierz do oceny ryzyka pozwala na określenie poziomu ryzyka. Zidentyfikowane zostały trzy poziomy ryzyka: niskie, średnie i wysokie. Zależność ryzyka od parametrów „prawdopodobieństwo" i „skutki" obrazuje poniższa tabela:

Poziom	Wartość
Wysokie	Większe lub równe 4,25
Średnie	Większe lub równe 1,2
Niskie	Większe lub równe 0

Przyjmuje się następujące podejście do akceptowania ryzyka:

Poziom ryzyka	
Wysokie	Ryzyko nieakceptowalne. Akceptacja możliwa jest decyzją Wójta. Wymaga natychmiastowego zaplanowania i podjęcia działania.
średnie	Ryzyko nieakceptowalne. Akceptacja możliwa jest decyzją Właściciela ryzyka. Wymaga zaplanowania działania.
Niskie	Ryzyko akceptowalne. Nie wymaga planowania i podejmowania działania.

6. Zaplanowanie działań związanych z analizowanym ryzykiem jest konieczne w przypadku, kiedy ryzyko nie jest akceptowalne. Należy wtedy stworzyć Plan postępowania z ryzykiem określając jakie działania zostaną podjęte, kto będzie odpowiedzialny za ich realizację i do kiedy mają zostać zrealizowane.
7. Następnie zalecane jest ocena ryzyka rezydualnego, czyli poziomu ryzyka po realizacji planu postępowania z ryzykiem i wprowadzeniu zabezpieczeń. Aby tego dokonać należy oszacować rezydualne prawdopodobieństwo i rezydualny skutek. Jeżeli ryzyko rezydualne nie jest akceptowalne, należy dokonać modyfikacji planu postępowania z ryzykiem i ponowić ocenę ryzyka rezydualnego.
8. Ostatnim krokiem jest opracowanie raportu z analizy ryzyka, przedstawienie go Wójtowi oraz udokumentowanie decyzji o postępowaniu z ryzykiem, właścicieli działań, terminów, ryzyka rezydualnego i statusu realizacji zabezpieczeń.

V. Przegląd i aktualizacja Procedury

1. Przegląd niniejszej Procedury jest wykonywany co najmniej raz w roku w ramach prac Komitetu Bezpieczeństwa oraz bezzwłocznie w przypadkach powodujących konieczność przeglądu SZBI zgodnie z Załącznikiem nr 4 do ustawy o KSC.
2. W przypadku zmiany przepisów lub istotnej zmiany kontekstu działania należy niezwłocznie dokonać przeglądu niniejszej Procedury oraz jeżeli istnieje taka potrzeba dokonać jej aktualizacji.
3. Za aktualizację niniejszej Procedury odpowiada Pełnomocnik ds. BI i CD.
4. Każda zmiana Procedury musi zostać udokumentowana.

Załącznik 1 - katalog zagrożeń zgodny z wytycznymi zawartymi w normy ISO 27005:2021 oraz ISO 27799

Lp.	Kategoria ryzyka	Zagrożenie
1	Zagrożenia fizyczne	Ogień
2	Zagrożenia fizyczne	Woda
3	Zagrożenia fizyczne	Zanieczyszczenia, szkodliwe promieniowanie
4	Zagrożenia fizyczne	Poważny wypadek
5	Zagrożenia fizyczne	Eksplozja
6	Zagrożenia fizyczne	Pył, korozja, zamarzanie
7	Zagrożenia naturalne	Zjawisko klimatyczne
8	Zagrożenia naturalne	Zjawisko sejsmiczne
9	Zagrożenia naturalne	Zjawisko wulkaniczne
10	Zagrożenia naturalne	Zjawisko meteorologiczne
11	Zagrożenia naturalne	Powódź
12	Zagrożenia naturalne	Zjawisko pandemii / epidemii
13	Awarie infrastruktury	Awaria systemu zasilania
14	Awarie infrastruktury	Awaria chłodzenia lub wentylacji
15	Awarie infrastruktury	Utrata zasilania
16	Awarie infrastruktury	Awaria sieci telekomunikacyjnej
17	Awarie infrastruktury	Awaria sprzętu telekomunikacyjnego
18	Awarie infrastruktury	Promieniowanie elektromagnetyczne
19	Awarie infrastruktury	Promieniowanie cieplne
20	Awarie infrastruktury	Impulsy elektromagnetyczne
21	Awarie techniczne	Uszkodzenie urządzenia lub systemu
22	Awarie techniczne	Przeciążenie systemu informacyjnego
23	Awarie techniczne	Naruszenie możliwości utrzymania systemu informacyjnego
24		
25	Działania ludzkie	Atak terrorystyczny, sabotaż
26	Działania ludzkie	Inżynieria społeczna
27	Działania ludzkie	Przechwytywanie promieniowania urządzenia
28	Działania ludzkie	Zdalne szpiegowanie
29	Działania ludzkie	Podsłuch
30	Działania ludzkie	Kradzież nośników lub dokumentów
31	Działania ludzkie	Kradzież sprzętu
32	Działania ludzkie	Kradzież tożsamości cyfrowej lub danych uwierzytelniających
33	Działania ludzkie	Odzyskiwanie nośników poddanych recyklingowi lub wyrzuconych.
34	Działania ludzkie	Ujawnianie informacji
35	Działania ludzkie	Dane wprowadzane z niewiarygodnych źródeł
36	Działania ludzkie	Manipulowanie przy urządzeniach
37	Działania ludzkie	Ingerencja w oprogramowanie
38	Działania ludzkie	Eksploity typu drive-by-exploits wykorzystujące komunikację internetową
39	Działania ludzkie	Atak typu replay, atak typu man-in-the-middle
40	Działania ludzkie	Nieuprawnione przetwarzanie danych osobowych
41	Działania ludzkie	Nieuprawnione wejście do obiektów
42	Działania ludzkie	Nieuprawnione użycie urządzeń
43	Działania ludzkie	Niewłaściwe użycie urządzeń

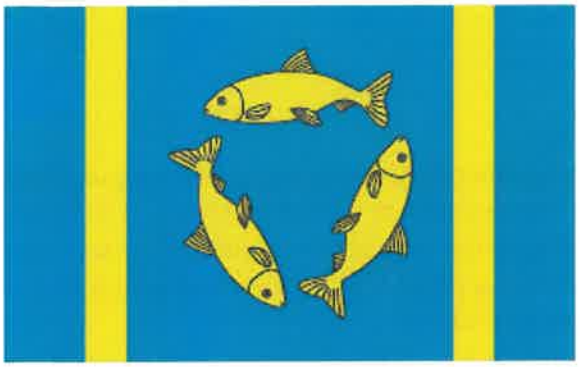
44	Działania ludzkie	Uszkodzenie urządzeń lub nośników
45	Działania ludzkie	Nielegalne kopiowanie oprogramowania
46	Działania ludzkie	Używanie podrobionego lub skopiowanego oprogramowania
47	Działania ludzkie	Uszkodzenie danych
48	Działania ludzkie	Nielegalne przetwarzanie danych
49	Działania ludzkie	Wysyłanie lub rozpowszechnianie złośliwego oprogramowania
50	Działania ludzkie	Wykrywanie położenia
51	Kompromitacja funkcji lub usług	Błąd w użyciu
52	Kompromitacja funkcji lub usług	Nadużywanie praw lub uprawnień
53	Kompromitacja funkcji lub usług	Fałszowanie praw lub uprawnień
54	Kompromitacja funkcji lub usług	Zaprzeczanie działaniom
55	Zagrożenia organizacyjne	Brak personelu
56	Zagrożenia organizacyjne	Brak zasobów
57	Zagrożenia organizacyjne	Niewydolność dostawców usług
58	Zagrożenia organizacyjne	Naruszenie prawa lub przepisów

Dodatkowo przy określaniu zagrożeń dla bezpieczeństwem informacji dotyczących stanu posiadania mieszkańców Gminy wykorzystywany jest również katalog 25 zagrożeń wynikających z normy ISO 27799, tj.:

1. Podszywanie się przez insajderów (np. pracowników i personel pomocniczy (stażyści) np. polegające na korzystaniu z systemu przez osoby wykorzystujące konta, które nie są ich własnymi).
2. Podszywanie się przez dostawców usług.
3. Podszywanie się przez osoby z zewnątrz (np. hakerów przy wykorzystaniu tzw. inżynierii społecznej).
4. Nieuprawnione wykorzystanie aplikacji związanych z informacjami dotyczącymi stanu posiadania mieszkańców Gminy.
5. Wprowadzanie szkodliwego lub zakłócającego oprogramowania.
6. Nadużycie zasobów systemowych.
7. Infiltracja komunikacji (wewnętrznej, zewnętrznej).
8. Przechwytywanie komunikatów.
9. Repudiowanie (zagrożenie to obejmuje użytkowników zaprzeczających, że wysłali wiadomość, czyli zaprzeczenie pochodzenia oraz użytkowników zaprzeczających, że otrzymali wiadomość, czyli zaprzeczenie odbioru np. brak potwierdzenia odbioru wiadomości e-mail).
10. Awaria połączenia.
11. Osadzenie złośliwego kodu.
12. Przypadkowy błąd w dostarczaniu (zagrożenie to obejmuje możliwość dostarczenia informacji pod niewłaściwy adres np. podczas przesyłania jej przez sieć).
13. Awaria techniczna hosta, magazynu danych lub infrastruktury sieciowej (zagrożenia te obejmują awarie sprzętu, awarie sieci lub awarie urządzeń służących do przechowywania danych).
14. Awaria wsparcia środowiskowego (w tym awarie zasilania i zakłócenia usług wynikające
    z klęsk żywiołowych lub spowodowanych przez człowieka).

15. Awaria oprogramowania systemowego lub sieciowego.
16. Awaria oprogramowania aplikacyjnego.
17. Błąd operatora.
18. Błąd konserwacji (Błędy popełniane przez osoby odpowiedzialne za utrzymanie sprzętu i oprogramowania systemowego).
19. Błąd użytkownika (błędy użytkowników mogą na przykład spowodować wysłanie poufnych informacji do niewłaściwego odbiorcy).
20. Niedobór pracowników (zagrożenie niedoborem pracowników obejmuje możliwość braku kluczowych pracowników i trudności z ich zastąpieniem).
21. Kradzież informacji przez osoby mające dostęp do informacji poufnych (w tym kradzież sprzętu lub danych).
22. Kradzież przez osoby postronne (w tym kradzież sprzętu lub danych).
23. Umyślne wyrządzenie szkody przez osoby mające dostęp do informacji poufnych (np. akty wandalizmu).
24. Umyślne wyrządzenie szkody przez osoby postronne.
25. Terroryzm.





DOKUMENT SYSTEMU ZARZĄDZANIA

BEZPIECZEŃSTWEM INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

Procedura zarządzania incydentami

Nazwa dokumentu	**Procedura zarządzania incydentami**
Autor dokumentu	Joanna Mrowicka
Sprawdzająca dokument	Aneta Skrzypczak-Kurzawa
Wersja dokumentu	0.2
Zatwierdzający dokument	Wójt Gminy
Data zatwierdzenia dokumentu	15 września 2026r.

I. Cel i zakres dokumentu

1. Celem opracowania i wdrożenia niniejszej Procedury jest konieczność uregulowania procesu zarządzania zdarzeniami oraz incydentami w Urzędzie Gminy Chrzypsko Wielkie tak, aby w przypadku wystąpienia incydentu zminimalizować jego negatywny wpływ na działalność prowadzoną przez Urząd oraz zmniejszyć ryzyko wystąpienia podobnego incydentu w przyszłości.
2. Procedura reguluje proces zarządzania zdarzeniami i incydentami w następujących obszarach:
   a) bezpieczeństwo (informacji, fizyczne, osobowe, techniczne i środowiskowe);
   b) ciągłość działania.
3. Zarządzanie incydentami stanowi element SZBI wymaganego dla podmiotu ważnego będącego podmiotem publicznym na podstawie art. 8 ust. 3 oraz Załącznika nr 4 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20, 252, 815, z późn. zm.). Normy PN-ISO/IEC 27001, PN-ISO/IEC 27002 i PN-ISO/IEC 27005 są stosowane pomocniczo.
   1) PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń;
   2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem.
4. Dokument obowiązuje we wszystkich lokalizacjach i komórkach organizacyjnych Urzędu Gminy i obowiązuje wszystkich pracowników Urzędzie.

II. Role i odpowiedzialności

1. **Kierownik Urzędu (Wójt)** odpowiada za:
   a) zapewnienie odpowiednich zasobów technicznych i organizacyjnych w celu zminimalizowania ryzyka wystąpienia incydentu lub minimalizacji negatywnych skutków incydentów, jeżeli miał miejsce;
   b) podejmowanie decyzji dotyczącej zarządzania incydentami – w tym podjęcie decyzji o zgłoszeniu incydentu do właściwego CSIRT sektorowego i/lub do organów ścigania;
   c) informowanie organów ścigania w przypadku incydentów z obszaru bezpieczeństwa jeśli zdarzenie miało/mogło mieć charakter kryminalny, sabotażowy, szpiegowski lub terrorystyczny.
   d) ponoszenie odpowiedzialności za wykonywanie obowiązków z zakresu cyberbezpieczeństwa również w przypadku powierzenia ich realizacji innej osobie za jej zgodą, zgodnie z art. 8c ustawy o KSC;
   e) zapewnienie, aby osoby realizujące zadania, o których mowa w art. 8 lub art. 11 ustawy o KSC, zostały dopuszczone do tych zadań po spełnieniu wymogu określonego w art. 8f ustawy o KSC, z uwzględnieniem równoważności ważnego poświadczenia bezpieczeństwa do informacji niejawnych o klauzuli „poufne" lub wyższej;
2. **Pełnomocnik ds. BI i CD** odpowiada za:
   a) rejestrowanie wszystkich otrzymanych Raportów o incydentach w obszarze funkcjonalnym BI i CD;
   b) klasyfikację incydentów zgodnie z załącznikiem nr 3,
   c) koordynowanie procesu zarządzania incydentami w obszarze funkcjonalnym BI i CD;
   d) przygotowywanie całościowych rekomendacji, wniosków i rozwiązań dotyczących powstałych incydentów.
3. **Inspektor Ochrony Danych** – odpowiada za ocenę incydentów pod kątem naruszenia ochrony danych osobowych oraz naruszenia praw i wolności osób, których dane dotyczą.

4. **Koordynator ds. bezpieczeństwa osobowego, budowy świadomości i szkoleń** – odpowiada za:
   a) rejestrowanie wszystkich otrzymanych Raportów o incydentach w obszarze bezpieczeństwa osobowego,;
   b) reagowanie na wszelkie incydenty z obszaru bezpieczeństwa osobowego;
   c) klasyfikację incydentów zgodnie z załącznikiem nr 3,
   d) przekazywanie informacji o incydentach Pełnomocnikowi ds. BI i CD;
   e) koordynowanie procesu zarządzania incydentami w tym zabezpieczenie dowodów do dalszego postępowania.
5. **Koordynatorzy ds. bezpieczeństwa technicznego, środowiskowego i fizycznego** odpowiada za:
   a) rejestrowanie wszystkich otrzymanych Raportów o incydentach w swoich obszarach funkcjonalnych;
   b) reagowanie na wszelkie incydenty w swoich obszarach funkcjonalnych we współdziałaniu z zakontraktowaną służbą ochrony fizycznej oraz innymi komórkami organizacyjnymi Urzędu Gminy poprzez wprowadzanie działań korekcyjnych i korygujących;
   c) klasyfikację incydentów zgodnie z załącznikiem nr 3;
   d) przekazywanie informacji o incydentach Pełnomocnikowi ds. BI i CD;
   e) koordynowanie procesu zarządzania incydentami w tym zabezpieczenie dowodów do dalszego postępowania.
6. **Wewnętrzne struktury cyberbezpieczeństwa** odpowiadają za:
   a) wsparcie osoby wyznaczonej do kontaktów z CSIRT w procesie informowania właściwego CSIRT sektorowego w przypadku incydentów z obszaru cyberbezpieczeństwa;
   b) reagowanie na incydenty w trybie rzeczywistym;
   c) przygotowywanie ostrzeżeń, rekomendacji i wniosków dotyczących możliwości wystąpienia incydentów a w przypadku wystąpienia incydentu przygotowanie raportu dotyczącego zdarzenia oraz podjętych/podejmowanych działań;
   d) klasyfikację incydentów zgodnie z załącznikiem nr 3;
   e) zabezpieczenie dowodów do dalszego postępowania;
   f) przekazywanie informacji o incydentach Pełnomocnikowi ds. BI i CD;
7. **Osoba zatrudniona na stanowisku ds. informatyki** / Administrator Systemów Informatycznych odpowiada za:
   a) analizę przyczyny wystąpienia incydentów w systemach informacyjnych oraz rekomendowanie środków mających na celu ich usunięcie;
   b) rekomendowanie działań minimalizujących skutki wystąpienia incydentu w systemach informacyjnych;
   c) przekazywanie informacji o incydentach Pełnomocnikowi ds. BI i CD;
   d) zabezpieczania dowodów cyfrowych.
8. **Pracownicy Urzędu - odpowiadają za:**
   a) zgłaszanie incydentów zgodnie z obowiązującymi Procedurami;
   b) współpracę z poszczególnymi osobami, zespołami, komórkami organizacyjnymi w zakresie zarządzania incydentami.
9. **Komitet Bezpieczeństwa odpowiada za:**
   a) ocenę i analizę incydentu jeżeli incydent wpływa lub może wpływać negatywnie na dwa lub więcej obszarów funkcjonalnych i znajduje się w zakresie obowiązków Pełnomocnika ds. BI i CD;

b) przedstawienie rekomendacji Kierownikowi Urzędu co do dalszego postępowania z incydentem;
c) przyjęcie roli komórki zarządzania kryzysowego w sytuacji zaistnienia incydentu krytycznego lub sytuacji kryzysowej oraz wsparcie Kierownictwa Urzędu w zarządzaniu Urzędem i Gminą w sytuacji kryzysowej.

10. **Osoba wyznaczona do kontaktów z CSIRT** odpowiada za:
    a) przygotowanie zgłoszenia o incydencie do CSIRT,
    b) utrzymywanie kontaktu z właściwym CSIRT sektorowym oraz z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie powierzonych zadań, z uwzględnieniem art. 9 ust. 3 ustawy o KSC;
    c) przekazywanie, w imieniu Urzędu, zgłoszeń incydentów poważnych do właściwego CSIRT sektorowego niezwłocznie, nie później niż w ciągu 72 godzin od momentu ich wykrycia, chyba że obowiązek zgłoszenia realizuje jednostka wyznaczona w ramach wspólnej obsługi cyberbezpieczeństwa;
    d) spełnienie - jeżeli osoba ta realizuje zadania, o których mowa w art. 8 lub art. 11 ustawy o KSC - przed rozpoczęciem tych zadań wymogu określonego w art. 8f ustawy o KSC;
    e) udział w szkoleniach i działaniach podnoszących świadomość cyberbezpieczeństwa zgodnie z programem szkoleń Urzędu; jeżeli osobie tej powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa, odbywa ona raz w roku kalendarzowym udokumentowane szkolenie, o którym mowa w art. 8e ustawy o KSC.

III. Zgłaszanie incydentów

1. Każdy pracownik oraz współpracownik Urzędu Gminy jest zobowiązany do zgłoszenia podejrzenia wystąpienia lub stwierdzenia wystąpienia incydentu.
2. Zgłoszenie podejrzenia wystąpienia lub stwierdzenie wystąpienia incydentu powinno zostać przekazane niezwłocznie (w ciągu 2h od stwierdzenia).
3. Zgłoszenia incydentów przyjmowane są całodobowo przez wyznaczone osoby lub system HelpDesk.
4. Zgłoszenia, o którym mowa powyżej, można dokonać:
    a) Telefonicznie – pod numerem: 61 295 10 11, 690 844 911.
    b) Osobiście – u Pełnomocnika ds. BI i CD, IODO, osoby wyznaczonej do kontaktów z wewnętrznej struktury cyberbezpieczeństwa lub wyznaczonej osoby do przyjmowania informacji na temat incydentów z obszaru bezpieczeństwa fizycznego;
    c) E-mailowo – urzad@chrzypsko.pl; informatyk@chrzypsko.pl
    d) Elektroniczna skrzynka podawcza - /4fflan664z/skrytka/
    e) E-doręczenia: AE:PL-64773-21728-SBJJD-24
    f) Poprzez system Help Desk – dotyczy zdarzeń z obszaru bezpieczeństwa IT.
5. Zgłoszenie w miarę możliwości powinno zawierać:
    a) opis incydentu,
    b) dane kontaktowe do osoby zgłaszającej wystąpienie incydentu lub podejrzenia wystąpienia incydentu,
    c) dane kontaktowe do świadków / uczestników incydentu
    d) obszar, którego dotyczy incydent (np. cyberbezpieczeństwo),
    e) rodzaj informacji,
    f) wskazanie, czy w związku z incydentem doszło do przerwania możliwości realizacji zadań publicznych lub świadczenia usług publicznych lub czy w skutek rozwoju incydentu zachodzi taka możliwość,
    g) datę wystąpienia lub podejrzenia wystąpienia incydentu,

h) datę wykrycia incydentu (jeżeli dotyczy),
i) przyczynę lub możliwe przyczyny wystąpienia incydentu,
j) możliwe skutki wystąpienia incydentu,
k) działania podjęte w związku ze stwierdzeniem wystąpienia lub podejrzeniem wystąpienia incydentu.

6. Zaleca się, aby pracownik oraz współpracownik dokonywał zgłoszenia za pomocą formularza zgłoszenia incydentu stanowiącego załącznik nr 1 do niniejszej Procedury.
7. Przykładowe zdarzenia podlegające zgłoszeniu znajdują się w załączniku nr 5 do niniejszej Procedury.
8. Pracownik i współpracownik Urzędu Gminy, dokonując zgłoszenia ma obowiązek poinformować o w/w zgłoszeniu swojego bezpośredniego przełożonego.
9. Brak zgłoszenia wystąpienia lub podejrzenia wystąpienia incydentu przez pracownika i współpracownika Urzędu Gminy może rodzić konsekwencje prawne. W szczególności brak zgłoszenia incydentu może skutkować odpowiedzialnością dyscyplinarną pracownika Urzędu Gminy lub odpowiedzialnością odszkodowawczą współpracownika Urzędu Gminy.
10. Wszystkie osoby obsługujące incydent mają prawo żądać od innych komórek organizacyjnych, pracowników i współpracowników Urzędzie Gminy przekazania dodatkowych informacji dotyczących incydentu. Wskazane informacje należy przekazywać bezzwłocznie.

IV. Zarządzanie incydentami

1. Pracownik obsługujący określony punkt kontaktowy do zgłaszania zdarzeń/ incydentów jest odpowiedzialny jest za przyjęcie zgłoszenia o incydencie.
2. Pracownik obsługujący określony punkt kontaktowy do zgłaszania zdarzeń/ incydentów po otrzymaniu i zarejestrowaniu zgłoszenia, przekazuje wszelkie zebrane informacje do osób, zespołów, komórek organizacyjnych odpowiedzialnych za dany obszar w Urzędzie Gminy (np. do komórki odpowiedzialnej za obszar IT), przy czym bez względu na obszar, informację o incydentach otrzymuje także zawsze Pełnomocnik ds. BI i CD.
3. Pracownik obsługujący określony punkt kontaktowy do zgłaszania zdarzeń/ incydentów w przypadku wstępnej klasyfikacji incydentu jako incydentu zagrażającego bezpieczeństwu przetwarzanych w Urzędzie Gminy informacji lub zagrażającemu ciągłości działania sporządza Raport z incydentu zgodnie z załącznikiem nr 4 i przesyła Raport Pełnomocnikowi ds. BI i CD.
4. Pełnomocnik z danego obszaru funkcjonalnego rejestruje wszystkie otrzymane Raporty i/lub informacje o incydentach, dokonuje ich klasyfikacji oraz informuje Kierownika Urzędu i jeśli wymaga tego sytuacja odpowiednie organy zewnętrzne (regulujące).
5. W przypadku incydentu dotykającego co najmniej dwa obszary funkcjonalne Pełnomocnik ds. BI i CD zwołuje obrady Komitetu Bezpieczeństwa.

V. Szczegółowa analiza incydentów

1. Zarejestrowane incydenty zagrażające bezpieczeństwu informacji, bezpieczeństwu fizycznemu w sposób krytyczny (zamach terrorystyczny/sabotażowy) lub zagrażające ciągłości działania Urzędu Gminy są analizowane przez Komitet Bezpieczeństwa.
2. Do analizy mogą być włączone inne osoby odpowiedzialne na poszczególne obszary działalności Urzędu Gminy jeśli tego wymaga sytuacja, poza osobami na stałe zasiadającymi w Komitecie Bezpieczeństwa.

3. Przy dokonywaniu oceny incydentu, osoby przeprowadzające analizę – weryfikują wpływ incydentu na działalność Urzędu Gminy, określają warianty następstw incydentu dla działalności Urzędu w przyszłości, przyczyny wystąpienia incydentu, zakres incydentu, określają również działania mające zminimalizowanie negatywnych skutków incydentu.
4. Wyniki analizy – oceny incydentu są dokumentowane i przechowywane przez Pełnomocnika ds. BI i CD lub przez Przewodniczącego Komitetu Bezpieczeństwa jeżeli Komitet został powołany.
5. Działania korekcyjne i korygujące związane z incydentem są prowadzone zgodnie z Procedurą działań korygujących.
6. Wszystkie incydenty mające miejsce w Urzędzie Gminy są badane raz na kwartał przez Pełnomocnika ds. BI i CD w celu wykrycia ewentualnych trendów lub przyczyn źródłowych ryzyk, które mogą skutkować wystąpieniem poważnego incydentu w przyszłości.
7. Dane z analizy, o której mowa powyżej stanowią dane wejściowe do analizy ryzyka i przeglądu zarządzania.

VI. Obsługa i zgłaszanie incydentów w zakresie cyberbezpieczeństwa

1. Zgłoszenia dotyczące cyberbezpieczeństwa przekazuje się drogą elektroniczną za pomocą systemu teleinformatycznego właściwego dla krajowego systemu cyberbezpieczeństwa. W razie braku możliwości skorzystania z tego systemu stosuje się sposób przekazywania zgłoszeń ogłoszony przez właściwy CSIRT zgodnie z ustawą o KSC.
2. Po otrzymaniu zgłoszenia Pełnomocnik ds. BI i CD oraz osoba odpowiedzialna za informatykę niezwłocznie rejestrują zdarzenie, podejmują działania ograniczające jego skutki i zabezpieczają materiał dowodowy, w szczególności logi, dane z systemów monitorujących, obrazy systemów, kopie konfiguracji, zdjęcia i inne dane istotne dla wyjaśnienia zdarzenia.
3. Incydent jest klasyfikowany na podstawie obowiązujących przepisów i aktualnych progów uznawania incydentu za poważny. O wyniku klasyfikacji, a także o incydentach mogących mieć istotny wpływ na realizację zadań publicznych, niezwłocznie informuje się Wójta.
4. Incydent zakwalifikowany jako poważny zgłasza się do właściwego CSIRT sektorowego niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia, zgodnie z art. 11 ust. 1 pkt 4a ustawy o KSC. Jeżeli zadania właściwego CSIRT sektorowego zostały powierzone CSIRT NASK, zgłoszenie kieruje się do CSIRT NASK. Urząd na bieżąco weryfikuje właściwość CSIRT i obowiązujący kanał zgłoszeniowy.
5. Jako podmiot ważny będący podmiotem publicznym Urząd, na podstawie art. 12c ustawy o KSC, nie przekazuje odrębnego wczesnego ostrzeżenia, sprawozdania okresowego, sprawozdania z postępu obsługi incydentu ani sprawozdania końcowego.
6. Zgłoszenie incydentu poważnego zawiera informacje znane w chwili zgłoszenia, w szczególności opis wpływu incydentu na realizowane zadanie publiczne lub świadczoną usługę, liczbę użytkowników dotkniętych skutkami, zasięg geograficzny, wpływ na inne podmioty, opis przyczyn i przebiegu incydentu oraz jego prawdopodobnych skutków, a także informacje o podjętych działaniach zapobiegawczych i naprawczych. Informacje są uzupełniane w toku obsługi incydentu, gdy stają się dostępne.
7. Informacje stanowiące tajemnice prawnie chronione przekazuje się wyłącznie w niezbędnym zakresie i odpowiednio oznacza. Na żądanie właściwego CSIRT

sektorowego Urząd uzupełnia zgłoszenie o informacje konieczne do realizacji zadań CSIRT.

8. Jeżeli występuje poważne cyberzagrożenie mogące oddziaływać na użytkowników usług Urzędu, informuje się ich o możliwych środkach zapobiegawczych, a gdy nie zwiększa to poziomu ryzyka - również o samym cyberzagrożeniu. O incydencie poważnym informuje się użytkowników, jeżeli ma on niekorzystny wpływ na świadczenie usług.
9. W przypadku wezwania do usunięcia podatności, która doprowadziła lub mogłaby doprowadzić do incydentu poważnego albo krytycznego, Pełnomocnik ds. BI i CD i osoba odpowiedzialna za informatykę niezwłocznie informują Wójta, planują działania naprawcze i dokumentują ich wykonanie oraz komunikację z właściwym organem i CSIRT.
10. Jeżeli obowiązki z zakresu cyberbezpieczeństwa są realizowane w ramach wspólnej obsługi albo przez jednostkę wyznaczoną zgodnie z art. 16e-16h ustawy o KSC, Urząd i jednostki obsługiwane przekazują jednostce wyznaczonej informacje o incydentach w terminach przez nią określonych, a jednostka wyznaczona realizuje zgłoszenia w imieniu podmiotów objętych wspólną obsługą.
11. Po zakończeniu obsługi incydentu sporządza się udokumentowaną analizę przyczyn, skutków, skuteczności reakcji i zabezpieczeń oraz ustala działania korygujące i doskonalące. Wnioski z incydentu stanowią dane wejściowe do szacowania ryzyka, przeglądu SZBI, aktualizacji planów ciągłości działania i programu szkoleń.

VII. Przeglądy oraz aktualizacja Procedury

1. Przegląd niniejszej Procedury jest dokonywany co najmniej raz w roku, a także bezzwłocznie po zmianie przepisów, rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa dotyczącej systemów lub usług ICT Urzędu, po wystąpieniu okoliczności mogących wpłynąć na ryzyko incydentu poważnego oraz po incydencie wskazującym na potrzebę zmiany procesu reagowania.
2. W przypadku zmiany przepisów lub istotnej zmiany kontekstu działania należy niezwłocznie dokonać przeglądu niniejszej Procedury oraz jeżeli istnieje taka potrzeba dokonać jej aktualizacji.
3. Za aktualizację niniejszej Procedury odpowiada Pełnomocnik ds. BI i CD, który powołuje Komitet Bezpieczeństwa w tym celu.
4. Każda zmiana Procedury musi zostać udokumentowana.

VIII. Wykaz załączników

1. Załącznik nr 1 – Formularz zgłoszenia incydentu
2. Załącznik nr 2 - Rejestr incydentów
3. Załącznik nr 3 - Klasyfikacja incydentów poważnych zgodnie z ustawą o KSC
4. Załącznik nr 4 - Raport z incydentu
5. Załącznik nr 5 – Katalog przykładowych zdarzeń podlegających zgłoszeniu

Załącznik nr 1

Formularz zgłoszenia incydentu

INFORMACJE PODSTAWOWE			
1. Dane kontaktowe osoby zgłaszającej	▪ Imię i nazwisko oraz stanowisko -jeżeli dotyczy		
	▪ Dane kontaktowe np. numer telefonu, adres e-mail		
2. Data i godzina wystąpienia zdarzenia/incydentu			
3. Data i godzina wykrycia zdarzenia/incydentu			
Opis zdarzenia/incydentu			
4. Czy w związku ze zdarzeniem/incydentem doszło do utraty życia lub zdrowia ludzi?		☐Tak ☐Nie	Jeżeli TAK, kogo dotyczy zdarzenie:
5. Czy w związku ze zdarzeniem/incydentem doszło do przerwania ciągłości lub zakłócenia realizacji zadań publicznych lub świadczenia usług publicznych?		☐Tak ☐Nie	Jeżeli TAK, jakich procesów dotyczy zdarzenie:
6. Czy w związku ze zdarzeniem/incydentem doszło do naruszenia bezpieczeństwa przetwarzanych informacji? (np. ujawniono osobie nieuprawnionej dokumentację)		☐Tak ☐Nie	Jeżeli TAK, rodzajów danych dotyczy zdarzenie:
7. Czy w związku z incydentem doszło do zakłócenia działania Organizacji innego niż proces świadczenia usług?		☐Tak ☐Nie	Jeżeli TAK, proszę o wskazanie w jakim zakresie – które procesy zostały zakłócone
8. Czy zdarzenie/incydent jest związany z działaniem systemu e-Puap?		☐Tak ☐Nie	Jeżeli TAK, proszę o wskazanie w jakim zakresie
9. Dane kontaktowe do uczestników oraz świadków zdarzenia/incydentu			

10. Dotychczasowe działania podjęte w związku ze zdarzeniem/incydentem	
11. Faktyczne lub możliwe przyczyny wystąpienia zdarzenia/incydentu	
12. Faktyczne lub możliwe skutki wystąpienia zdarzenia/incydentu	
13. Podmioty, których również może dotyczyć zdarzenie/incydent	
14. Informacje dodatkowe	

Załącznik nr 2

Rejestr incydentów

Lp.	Incydent	Data wystąpienia incydentu	Data zgłoszenia incydentu	Klasyfikacja incydentu	Skutek incydentu	Opis incydentu	Przyczyna wystąpienia incydentu

Data zgłoszenia incydentu do odpowiedniego organu	Nazwa organu któremu zgłoszono incydent	Forma wykonania zgłoszenia / powiadomienia organu o incydencie	Podjęte działania korygujące	Jeżeli o incydencie nie powiadomiono organu należy krótko uzasadnić podjęta decyzję	Uwagi

Załącznik nr 3

Klasyfikacja incydentów poważnych

Lp.	Incydent poważny	Opis	Przykład
1	Incydent dotyczący systemów it dotyczących świadczenia usług na rzecz mieszkańców	1. liczba użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej: nie dotyczy; 2. czas oddziaływania incydentu na świadczoną usługę kluczową: incydent doprowadził do braku dostępności usługi powyżej 24 godzin; 3. zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4. inne czynniki charakterystyczne dla danego sektora lub podsektora: a) incydent doprowadził do braku poufności danych przetwarzanych w usłudze lub b) incydent doprowadził do braku integralności danych przetwarzanych w usłudze.	1. Brak dostępu do systemu informatycznego, prowadzący do braku możliwości realizacji zadań publicznych lub świadczenia usług publicznych gwarantowanych powyżej 24 godzin. 2. Nieuprawniona zmiana danych w systemie ED (brak integralności 3. Brak mediów (np. wody, prądu) prowadzący do braku możliwości realizacji zadań publicznych lub świadczenia usług publicznych gwarantowanych powyżej 24 godzin. 4. Brak personelu np. z powody strajku, epidemii skutkujący brakiem możliwości realizacji zadań publicznych lub świadczenia usług publicznych gwarantowanych powyżej 24 godzin.
2	Incydent o charakterze osobowym, dotyczący świadczenia usług na rzecz mieszkańców	1. liczba użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej: nie dotyczy; 2. czas oddziaływania incydentu na świadczoną usługę kluczową: incydent doprowadził do braku dostępności usługi powyżej 24 godzin; 3. zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4. inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu, c) inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby,	1. Brak dostępu do systemu informatycznego, prowadzący do braku możliwości realizacji zadań publicznych lub świadczenia usług publicznych powyżej 24 godzin. 2. Brak dostępu do systemu informatycznego skutkujący śmiercią. 3. Nieuprawniona zmiana danych w systemie (brak integralności dokumentacji). 4. Naruszenie poufności danych mieszkańców. 5. Brak mediów (np. wody, prądu) prowadzący do braku możliwości udzielania usług powyżej 24 godzin. 6. Brak personelu np. z powody strajku, epidemii skutkujący brakiem możliwości udzielania usług powyżej 24 godzin.

		d) brak poufności danych przetwarzanych w usłudze, e) brak integralności danych przetwarzanych w usłudze.	7. Awaria sprzętu
3	Incydent dotyczący gromadzenia i udostępniania Elektronicznej Dokumentacji	1. liczba użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej: nie dotyczy; 2. czas oddziaływania incydentu na świadczoną usługę kluczową: incydent doprowadził do braku dostępności usługi powyżej 1 godziny; 3. zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4. inne czynniki charakterystyczne dla danego sektora lub podsektora: a) incydent doprowadził do braku poufności danych przetwarzanych w usłudze lub b) incydent doprowadził do braku integralności danych przetwarzanych w usłudze.	1. Brak dostępu do systemu informatycznego służącego do gromadzenia i udostępniania ED, skutkujący brakiem możliwości świadczenia usług pow. 1 godziny. 2. Naruszenie poufności danych przetwarzanych w ramach systemu informatycznego służącego do gromadzenia i udostępniania ED. 3 Naruszenie integralności danych przetwarzanych w ramach systemu informatycznego służącego do gromadzenia i udostępniania ED.
4	Incydent dotyczący usług społecznych	1. liczba użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej: nie dotyczy; 2. czas oddziaływania incydentu na świadczoną usługę kluczową: incydent doprowadził do braku dostępności usługi powyżej 24 godzin; 3. zasięg geograficzny obszaru, którego dotyczy incydent: nie dotyczy; 4. inne czynniki charakterystyczne dla danego sektora lub podsektora: incydent spowodował co najmniej jedną z poniżej wymienionych okoliczności: a) śmierć człowieka, b) ciężki uszczerbek na zdrowiu, c) brak poufności danych przetwarzanych w usłudze, d) brak integralności danych przetwarzanych w usłudze.	1. Brak dostępu do systemu informatycznego, prowadzący do braku możliwości świadczenia usług powyżej 24 godzin. 2. Brak poufności danych w usłudze np. wyciek danych. 3. Brak integralności danych w usłudze np. nieautoryzowana zmiana danych.

Załącznik 4

Raport z incydentu

Raport z incydentu	
Imię i nazwisko oraz stanowisko osoby wypełniającej Raport	
Data sporządzenia Raportu	
Data i godzina zgłoszenia incydentu wraz ze wskazaniem organu, do którego zgłoszono incydent (jeżeli dotyczy)	
Opis incydentu	
Osoby, komórki, inne podmioty (np. podłączone do Platformy) powiadomione o incydencie	
Data i sposób zamknięcia incydentu (jeżeli dotyczy)	
Informacje o zgromadzonych materiałach	

dowodowych (jeżeli dotyczy)	
Informacje dotyczące dalszego sposobu postępowania z incydentem (jeżeli dotyczy)	
Podpis osoby wypełniającej Raport	

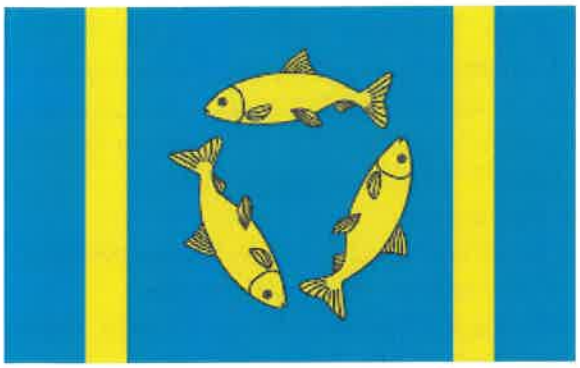
Załącznik nr 5

Katalog przykładowych zdarzeń podlegających zgłoszeniu

1. Zgubienie / kradzież / zniszczenie dokumentacji.
2. Wydanie lub przesłanie dokumentacji nieuprawnionej osobie.
3. Udzielanie informacji na temat stanu sprawy osobie nieuprawnionej.
4. Zgubienie kluczy lub kart dostępu do pomieszczeń.
5. Niezdanie kluczy do pomieszczeń po zakończonym dniu pracy.
6. Wniesienie prywatnego komputera do stref bezpiecznych.
7. Udostępnienie danych osobowych osobom nieuprawnionym.
8. Wejście / włamanie / osób nieuprawnionych do obszarów przeznaczonych wyłącznie dla pracowników Urzędzie Gminy oraz przebywanie osób nieuprawnionych w strefach przeznaczonych wyłącznie dla pracowników Urzędzie Gminy bez nadzoru.
9. Włamanie do pomieszczeń.
10. Włamanie do archiwum.
11. Włamanie do serwerowni.
12. Pozostawienie pomieszczenia, w którym są przetwarzane dane osobowe bez nadzoru.
13. Zgubienie / kradzież / zniszczenie nośnika informacji np. PENDRIVE zawierającego dane osobowe lub informacje chronione.
14. Zgubienie / kradzież / dokumentacji klasyfikowanej jako dokumentacja chroniona/stanowiącą tajemnicę Urzędu Gminy.
15. Nieuprawniona ingerencja w służbowy sprzęt elektroniczny (laptop, telefon komórkowy) celem pozyskania informacji.
16. Sprzedaż/ujawnienie osobom/podmiotom trzecim informacji wrażliwych / stanowiących tajemnicę Urzędu Gminy.
17. Próby indagowania pracowników/współpracowników Urzędzie Gminy na temat informacji wrażliwych / stanowiących tajemnicę Urzędu Gminy.
18. Instalacja złośliwego oprogramowania w systemie użytkownika.
19. Przesłanie wiadomości zawierającej poufne dane (np. dane osobowe pacjenta, umowę) niewłaściwej osobie.
20. Przypadkowe ujawnienie swojego loginu i hasła do systemu.
21. Niestabilność systemów oraz aplikacji teleinformatycznych.
22. Zbyt duże obciążenie podzespołów sprzętu teleinformatycznego.
23. Brak aktualnych kopii zapasowych.
24. Zidentyfikowanie prób omijania zabezpieczeń systemów teleinformatycznych.
25. Pożar w pomieszczeniu serwerowym.
26. Uszkodzenie stacji roboczej.
27. Zgubienie / kradzież / zniszczenie służbowego telefonu / laptopa.
28. Zidentyfikowanie nieznanych nośników lub urządzeń wpiętych do gniazd USB komputerów stacjonarnych, laptopów.
29. Nieautoryzowane wpięcie do okablowania infrastruktury teleinformatycznej.
30. Próby nieautoryzowanego lub nieautoryzowane przechwycenie przechwycenia sygnału lub pasma elektromagnetycznego z urządzeń systemu teleinformatycznego Urzędu Gminy.
31. Brak zachowania zasady czystego biurka, czystej drukarki (pozostawienie dokumentacji bez nadzoru w miejscu, do którego dostęp mogły posiadać osoby nieuprawnione do jej przetwarzania).
32. Brak zachowania zasady czystego pulpitu.
33. Niezablokowanie stacji roboczej przez Użytkownika oraz pozostawienie jej bez nadzoru w miejscu, do którego dostęp mogły posiadać osoby nieuprawnione do jej przetwarzania.

34. Inne zdarzenia losowe wynikające z zjawisk atmosferycznych, które zakłócą ciągłość działania i/lub możliwość świadczenia usług.

Wójt
mgr inż. Edmund Ziółek



DOKUMENT SYSTEMU ZARZĄDZANIA

BEZPIECZEŃSTWEM INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

Procedury bezpieczeństwa technicznego, środowiskowego i fizycznego

Nazwa dokumentu	**Procedury bezpieczeństwa technicznego, środowiskowego i fizycznego**
Autor dokumentu	Joanna Mrowicka
Sprawdzająca dokument	Aneta Skrzypczak-Kurzawa
Wersja dokumentu	0.2
Zatwierdzający dokument	Wójt Gminy
Data zatwierdzenia dokumentu	15 września 2026r.

I. Cel i zakres dokumentu

1. Celem opracowania i wdrożenia niniejszych Procedur jest określenie zasad i standardów zarządzania bezpieczeństwem fizycznym, technicznym i środowiskowym, w tym realizacja wymogu ochrony miejsc, w których przetwarzane są informacje, określonego w Załączniku nr 4 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20, 252, 815, z późn. zm.).
2. **Procedury określają podstawowe zasady dotyczące:**
   a. wydzielenia, zabezpieczenia i pracy w poszczególnych strefach bezpieczeństwa,
   b. stosowania zabezpieczeń fizycznych, technicznych i środowiskowych.
3. Procedury obowiązują we wszystkich komórkach Organizacyjnych Urzędu Gminy Chrzypsko Wielkie, zwanego dalej „Urzędem Gminy" lub „Urzędem".
4. Procedury obowiązują we wszystkich lokalizacjach i komórkach organizacyjnych Urzędu oraz obowiązują cały personel Urzędu.
5. Kierownicy jednostek organizacyjnych Gminy objętych wspólną obsługą cyberbezpieczeństwa stosują wymagania niniejszych Procedur w zakresie formalnie przyjętym dla danej jednostki albo wynikającym z decyzji jednostki wyznaczonej. Pozostałe jednostki zapewniają równoważne wymagania w swoim SZBI.

II. Role i odpowiedzialności

1. **Koordynator ds. bezpieczeństwa fizycznego, technicznego i środowiskowego** - odpowiada za:
   a) nadzór nad procesowaniem wyboru firmy świadczącej usługi ochrony fizycznej dla Urzędu;
   b) przygotowaniem systemu informowania o incydentach w zakresie ochrony fizycznej w tym wyznaczenie w systemie dyżurowym osób odpowiedzialnych za przyjmowanie zgłoszeń o incydentach w obszarze ochrony fizycznej;
   c) nadzór nad ochroną fizyczną;
   d) wyznaczenie osób do telefonicznego dyżuru 24/7 celem odbierania informacji na temat niepożądanych zdarzeń (incydentów) z zakresu bezpieczeństwa fizycznego,
   e) wyznaczenie stref bezpieczeństwa;
   f) nadzór nad zakupami potrzebnego sprzętu i wyposażenia w obszarze ochrony fizycznej;
   g) systematyczne przeglądy sprzętu i wyposażenia w obszarze ochrony fizycznej;
   h) przygotowanie procedur wydawani kluczy i jej systematyczny przegląd;
   i) nadzór nad system kontroli dostępu (SKD), systemem monitoringu przemysłowego (CCTV) oraz systemem sygnalizacji włamania i napadu (SSWiN);
   j) odpowiednie zabezpieczenie serwerowni i centrów przetwarzania danych – w tym za wnioskowanie o wprowadzenie dodatkowych zabezpieczeń;
   k) udział w obradach Komitetu Bezpieczeństwa;
   l) ścisłą współpracę z Pełnomocnikiem ds. BI i CD.
   m) odpowiednie rozłożenie okablowania w serwerowni;
   n) odpowiednie usytuowanie urządzeń niepowodujące nadmiernego nagrzewania się itp.,
   o) odpowiednie zabezpieczenie serwerowni i centrów przetwarzania danych pod względem technicznym i środowiskowym – w tym za wnioskowanie o wprowadzenie dodatkowych zabezpieczeń;
   p) ścisłą współpracę z Inspektorem ochrony ppoż. oraz Inspektorem BHP;
   q) koordynację działań dezynfekcji, dezynsekcji i deratyzacji;
   r) zapewnienie zasobów w zakresie bezpieczeństwa technicznego urządzeń teleinformatycznych (np. listew antyprzepięciowych, urządzeń UPS, podzespołów chłodzących itp.);
   s) aktualizację niniejszej procedury w koordynacji z Pełnomocnikiem ds. bezpieczeństwa informacji i ciągłości działania w obszarze bezpieczeństwa technicznego i środowiskowego.

2. **Inspektor Ochrony Danych (IOD)** odpowiada za współpracę z osobami odpowiedzialnymi za pracę poszczególnych komórek organizacyjnych oraz z Pełnomocnikiem ds. Bezpieczeństwa Informacji w zakresie wdrożenia odpowiednich środków zabezpieczeń danych osobowych w poszczególnych komórkach organizacyjnych.
3. **Pełnomocnik ds. Bezpieczeństwa Informacji i Ciągłości Działania** odpowiada za:
   a) przegląd i aktualizację Procedury bezpieczeństwa fizycznego, technicznego i środowiskowego;
   b) ścisłą współpracę z Koordynatorem ds. bezpieczeństwa technicznego, środowiskowego i fizycznego;
   c) doradzanie osobom odpowiedzialnym za pracę poszczególnych komórek organizacyjnych w zakresie wdrożenia dodatkowych środków zabezpieczeń;
   d) wnioskowanie o wdrożenie dodatkowych zabezpieczeń;
   e) systematyczny przegląd zabezpieczeń;
   f) monitorowanie przestrzegania zasad bezpieczeństwa fizycznego, technicznego i środowiskowego zgodnie z Procedurą.

4. **Inspektor ochrony PPOŻ**
   a) udziela wsparcia Koordynatorowi ds. bezpieczeństwa technicznego, środowiskowego i fizycznego w zakresie bezpieczeństwa technicznego i środowiskowego w swoim obszarze funkcjonalnym;
   b) bierze czynny udział w pracach i obradach Komitetu Bezpieczeństwa;
   c) wspiera Koordynatora ds. bezpieczeństwa technicznego, środowiskowego i fizycznego oraz Pełnomocnika ds. Bezpieczeństwa Informacji w zakresie zarządzania ryzykiem.
5. **Inspektor BHP**
   a) udziela wsparcia Koordynatorowi ds. bezpieczeństwa technicznego, środowiskowego i fizycznego w zakresie bezpieczeństwa technicznego i środowiskowego w swoim obszarze funkcjonalnym;
   b) bierze czynny udział w pracach i obradach Komitetu Bezpieczeństwa;
   c) wspiera Koordynatora ds. bezpieczeństwa technicznego, środowiskowego i fizycznego oraz Pełnomocnika ds. Bezpieczeństwa Informacji w zakresie zarządzania ryzykiem.
6. **Osoby odpowiedzialne za pracę poszczególnych komórek organizacyjnych** odpowiadają za:
   a) Stosowanie się do niniejszych Procedur,
   b) określają zasoby niezbędne do ochrony informacji,
   c) odpowiadają za wnioskowanie o wdrożenie dodatkowych środków zabezpieczeń,
   d) w zależności od obszaru odpowiadają za prowadzenie dokumentacji eksploatacyjnej poszczególnych zabezpieczeń fizycznych /technicznych /środowiskowych.
7. **Pracownicy Urzędu** odpowiadają za:
   a) stosowanie się do niniejszych Procedur,
   b) zgłaszanie przełożonym konieczności wprowadzenia dodatkowych zabezpieczeń.

III. Postanowienia ogólne

1. W Urzędzie Gminy ustanowiono wyraźny podział na dwa obszary funkcjonalne; bezpieczeństwo fizyczne oraz bezpieczeństwo techniczne i środowiskowe.
2. W odniesieniu do powyższego zapisu Kierownik Urzędu na podstawie decyzji lub innych zapisów wyznaczy Koordynator ds. bezpieczeństwa technicznego, środowiskowego i fizycznego.
3. Zakres środków bezpieczeństwa fizycznego, technicznego i środowiskowego jest definiowany na podstawie udokumentowanego szacowania ryzyka oraz wymogów

Załącznika nr 4 do ustawy o KSC, w szczególności ochrony miejsc przetwarzania informacji, kontroli uprawnień i zabezpieczenia dostępności systemów.

4. W przypadku korzystania z usług chmury obliczeniowej albo zewnętrznego centrum przetwarzania danych Urząd dokumentuje mechanizmy zapewniające ochronę przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniem i zakłóceniami oraz weryfikuje te mechanizmy w ramach nadzoru nad dostawcą.
5. Nośniki i urządzenia służące do wykonywania kopii zapasowych są chronione przed nieuprawnionym dostępem oraz - zgodnie z przyjętą architekturą kopii - odseparowane fizycznie i logicznie od danych przetwarzanych w systemach produkcyjnych. Lokalizacja i sposób przechowywania kopii podlegają okresowej weryfikacji.
6. Dostęp do stref chronionych, serwerowni, punktów dystrybucyjnych i innych miejsc przetwarzania informacji przyznaje się zgodnie z zasadą minimalnych uprawnień; uprawnienia są przeglądane, modyfikowane po zmianie zadań i bezzwłocznie cofane po ustaniu podstawy dostępu.
7. Bezpieczeństwo fizyczne, techniczne i środowiskowe jako jedna z domen bezpieczeństwa jest środkiem do uzyskania wysokich standardów bezpieczeństwa generalnie, a w szczególności bezpieczeństwa informacji i ciągłości działania i odporności na zagrożenia.
8. Dobrze zorganizowany proces bezpieczeństwa fizycznego ma w swojej istocie nie dopuścić do naruszenia istotnych/krytycznych zasobów Urzędzie Gminy.
9. W bezpieczeństwie fizycznym oraz technicznym należy w szczególności brać pod uwagę kontekst zewnętrzny Urzędu tak w wymiarze lokalnym, jak i globalnym, podczas szacowania ryzyka oraz w etapie wprowadzania zabezpieczeń. Do najważniejszych czynników podczas właściwego planowania bezpieczeństwa fizycznego zalicza się:
    a) wprowadzone stopnie alarmowe oraz możliwość ich wprowadzenia;
    b) znaczenie Urzędu w kontekście niepożądanych zdarzeń w wymiarze lokalnym jak i globalnym;
    c) inne zagrożenia w wymiarze państwowym – szpiegostwo, wojna, stan wojenny, zagrożenia sabotażowe;
    d) zagrożenia związane z lokalizacją Urzędu;
    e) zagrożenia naturalne;
    f) ilość niepożądanych zdarzeń w wymiarze bezpieczeństwa fizycznego w ostatnim założonym okresie czasu jak: wandalizm, napaści na urzędników, próby włamań, włamania, rozboje i kradzieże, inne.
10. Środki bezpieczeństwa fizycznego, technicznego i środowiskowego obejmują w szczególności:
    a) ustanowienie stref bezpieczeństwa,
    b) określenia sposobu zabezpieczenia wejścia do Urzędu oraz do stref bezpieczeństwa,
    c) stosowanie ochrony fizycznej,
    d) stosowanie zabezpieczeń instalacji elektrycznej,
    e) stosowania czujników dymu,
    f) stosowania mechanicznych zabezpieczeń (np. zamki, kraty w oknach),
    g) stosowanie urządzeń ochrony przeciwpożarowej,
    h) stosowanie zabezpieczeń przeciwprzepięciowych,
    i) stosowanie środków ochrony odgromowej,
    j) zabezpieczenie przed zalaniem wodą,
    k) zapewnienie właściwych warunków w zakresie temperatury i wilgotności powietrza,
    l) zabezpieczenie okablowania.
11. Pracownicy odpowiadają za wnioskowanie o wdrożenie koniecznych – w ich ocenie - dodatkowych środków zabezpieczeń.

12. Za prowadzenie i utrzymywanie dokumentacji eksploatacyjnej dotyczącej wdrożonych zabezpieczeń fizycznych, odpowiada Koordynator ds. bezpieczeństwa fizycznego.
13. Za prowadzenie i utrzymywanie dokumentacji eksploatacyjnej dotyczącej wdrożonych zabezpieczeń technicznych i środowiskowych, odpowiada Koordynator ds. bezpieczeństwa technicznego i środowiskowego w koordynacji z Inspektorem BHP oraz Inspektorem ochrony ppoż.
14. Dokumentacja informacyjna dotycząca wdrożonych zabezpieczeń (plany, schematy, specyfikacje techniczne) przechowywana jest w dwóch kopiach. Jedną kopię posiada Pełnomocnik ds. BI, drugą kopię posiada Koordynator ds. bezpieczeństwa fizycznego, technicznego i środowiskowego.

IV. Wytyczne bezpieczeństwa granic obszaru bezpiecznego

1. W Urzędzie są wyznaczone 3 strefy bezpieczeństwa:
   - 1.1 **Strefa ogólna (publiczna)**
     - 1.1.1 Strefa obejmuje: korytarze i punkt informacyjny, poczekalnie, hole wejściowe, ciągi komunikacyjne, teren otaczający budynek, ciągi komunikacyjne, parking.
     - 1.1.2 Dostęp do strefy jest nadzorowany w szczególności za pośrednictwem środków ochrony fizycznej.
     - 1.1.3 Dostęp do strefy posiadają wszystkie osoby znajdujące się na terenie danej lokalizacji (w tym osoby postronne), np.:
       a. wszyscy Pracownicy/Współpracownicy,
       b. Klienci,
       c. goście,
       d. dostawcy,
       e. interesanci,
       f. kurierzy, itp.
   - 1.2 **Strefa III - administracyjna**
     - 1.2.1 Strefa obejmuje: wszystkie obszary związane z działalnością Urzędu, które nie mają charakteru obszarów ogólnodostępnych (np. pomieszczenia takie jak: pokoje pracowników, pomieszczenia socjalne, pomieszczenia administracyjne, sekretariaty).
     - 1.2.2 Dostęp do strefy jest ograniczony i kontrolowany.
     - 1.2.3 Dostęp do strefy posiadają uprawnieni pracownicy i współpracownicy Urzędu.
     - 1.2.4 Osoby z zewnątrz mogą przebywać we wskazanej strefie pod nadzorem pracowników / współpracowników Urzędzie.
     - 1.2.5 W strefie wymagane jest zapewnienia podstawowych wymagań bezpieczeństwa w zakresie kontroli dostępu (np. zamykanie pomieszczeń na klucz) oraz w zakresie bezpieczeństwa (systemy przeciwpożarowe, systemy antywłamaniowe).
   - 1.3 **Strefa II i/lub Strefa I - chroniona**
     - 1.3.1 Strefa obejmuje: pomieszczenia zawierające nośniki, na których znajdują się wrażliwe informacje oraz informacje prawnie chronione (np. listy płac, umowy z kontrahentami, dokumenty zawierające dane osobowe, dane finansowo-księgowe, polityki i procedury bezpieczeństwa, inna dokumentacja chroniona). Strefa obejmuje w szczególności np. archiwa, kancelarie oraz pomieszczenia, w których znajdują się krytyczne urządzenia systemów IT, m.in. serwerownie, punkty dystrybucyjne, centra danych, węzły łączności.
     - 1.3.2 Dostęp do strefy jest ściśle nadzorowany i kontrolowany.
     - 1.3.3 Dostęp do wskazanej strefy posiadają wyłącznie uprawnieni pracownicy/współpracownicy Urzędu.
     - 1.3.4 Osoby trzecie mogą przebywać we wskazanej strefie pod ścisłym nadzorem pracowników/współpracowników Urzędzie.

1.3.5 W strefie wymagane jest zapewnienie podwyższonych wymagań bezpieczeństwa w zakresie kontroli dostępu (karty SKD, zamykanie pomieszczeń na klucz, odnotowywanie każdego wejścia oraz wyjścia – prowadzenie ewidencji) oraz w zakresie bezpieczeństwa (system przeciwpożarowy, system SSWiN, ochrona fizyczna, wzmocnione drzwi, klimatyzacja, kraty w oknach).

1.3.6 Sprzątanie pomieszczeń w strefie odbywa się w obecności pracownika/współpracownika Urzędu, uprawnionego do przebywania we wskazanej strefie.

2. Dostęp do poszczególnych stref jest przydzielany zgodnie z zasadami minimalizacji uprawnień oraz zasadą wiedzy koniecznej – co oznacza, że dostęp do strefy jest udzielany tylko osobom, którym dostęp ten jest niezbędny w celu realizacji zadań na rzecz Urzędu i tylko w czasie wykonywania tych zadań.
3. Przeprowadzane jest okresowe przeglądanie praw dostępu do stref chronionych.
4. Przegląd jest dokumentowany.
5. W każdej ze stref bezpieczeństwa – jeżeli wynika to z szacowania ryzyka – opracowuje się i wdraża szczegółowe zasady bezpieczeństwa oraz zapoznaje się z nimi osoby przebywające w danej strefie.
6. Każdy pracownik/współpracownik Urzędu jest zobowiązany do przestrzegania obowiązujących zasad w poszczególnych strefach.
7. Każdy pracownik/współpracownik Urzędu, odpowiada za gości i jest zobowiązany do zapoznania gości – tam, gdzie to właściwe – z zasadami bezpieczeństwa obowiązującymi w danej strefie.

V. Zasady dostępu do pomieszczeń biurowych i ochrony fizycznej

1. Ochrona osób i mienia realizowana jest w formie bezpośredniej ochrony fizycznej:
   a) stałej lub doraźnej,
   b) polegającej na stałym dozorze sygnałów przesyłanych, gromadzonych i przetwarzanych w elektronicznych urządzeniach i systemach alarmowych.
2. Ochrona fizyczna zasobów jest sprawowana przez przedsiębiorcę posiadającego koncesję na prowadzenie działalności gospodarczej w zakresie ochrony osób i mienia, wydaną przez Ministra właściwego do spraw wewnętrznych.
3. Za koordynację działań ochrony fizycznej ze strony Urzędu odpowiada Koordynator ds. bezpieczeństwa technicznego, środowiskowego i fizycznego.
4. Na wypadek zaistnienia incydentu z obszaru bezpieczeństwa fizycznego, Podmiot świadczący ochronę fizyczną zapewnia możliwość kontaktu ochrony fizycznej z wyznaczoną osobą lub osobami w systemie dyżurowym (telefonicznym) 24/7 .
5. W Urzędzie zastosowane zostały systemy zabezpieczenia technicznego:,
   a) ochrona przeciwpożarowa zasobów,
   b) listwy zabezpieczające napięcie elektryczne i bezpieczniki,
   c) czujnik dymu.
6. Dostęp do pomieszczeń jest chroniony przez system SKD lub klucze a dostępy nadawane zgodnie z ustalonymi profilami dostępów przypisanymi do stanowisk. Dopuszczalny jest również dostęp do pomieszczeń na klucz. Niedopuszczalne jest użyczanie kart dostępu osobom trzecim – w tym również współpracownikom.
7. W pomieszczeniach, w których ulokowane są kluczowe elementy infrastruktury teleinformatycznej, poza sytuacjami wyjątkowymi nie zezwala się osobom na fotografowanie, nagrywanie audio/video itp. Zgodę na odstępstwo w powyższym wyraża Wójt po wcześniejszej opinii Pełnomocnika ds. BI i CD.

VI. Zasady funkcjonowania i archiwizacji serwerowni

1. Decyzje w zakresie wprowadzania zabezpieczeń w serwerowni są poprzedzone szacowaniem ryzyka.

2. Podczas wprowadzania zabezpieczeń, bierze się pod uwagę m.in. wymagania i wytyczne wynikające z:
   a) TIA-942 Telecommunications Infrastructure Standard for Data Centers;
   b) Standard 90.4-2019 - Energy Standard for Data Centers (ANSI Approved);
   c) Standard 127-2012 - Method of Testing for Rating Computer and Data Processing Room Unitary Air Conditioners (ANSI Approved);
   d) ASHRAE: Design Consideration for Datacom Equipment Centers;
   e) Liquid Cooling Guidelines for Datacom Equipment Centers, Second Edition;
   f) Liquid Cooling Guidelines for Datacom Equipment Centers, Second Edition;
   g) Standardów ISO, w tym w szczególności: ISO 27001, ISO 22301, ISO/IEC 22237-1:2021, PN- HD 60364-4-41:2017-09, PN-EN 50172:2005, PN-EN 12464-2:2014-05, PN- EN 1838:2013-11, PN-EN 62305-1:2011, PN-EN 50310:2016-09, PN-HD 60364-1:2010, PN-HD 60364-4-442:2012, PN-HD 60364-4-444:2012 , PN-EN 50174-1:2018-08;
   h) ustawy z dnia 7 lipca 1994 r. - Prawo budowlane;
   i) jeśli właściwe jako dokument główny lub pomocniczy: Rozporządzenie Rady Ministrów z dnia 29 maja 2012r w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.
3. Układy chłodzenia stanowią kluczową część infrastruktury sieciowej, która warunkuje wysoki poziom dostępności systemów teleinformatycznych.
4. Na system chłodzenia składa ją się m.in.:
   a) agregaty zewnętrzne,
   b) urządzenia wewnętrzne,
   c) system sterowania.
5. Klimatyzacja jest kluczowym systemem służącym zapewnieniu właściwych parametrów środowiskowych, takich jak temperatura, wilgotność, czystość powietrza, wymaganych przez pracujący w serwerowni sprzęt teleinformatyczny. System chłodzenia w pomieszczeniu serwerowni musi być dostosowany do warunków pomieszczenia i mocy cieplnej wydzielanej przez zainstalowane w serwerowni urządzenia oraz należy uwzględnić również ciepło, które jest wydzielane przez pracowników wchodzących do serwerowni.

VII. Zasady bezpieczeństwa fizycznego, technicznego i środowiskowego

1. Zabezpieczenia zewnętrzne w danej lokalizacji powinny obejmować m.in. takie obszary jak zewnętrzne ciągi komunikacyjne – ciągi piesze, drogi dojazdowe, parkingi, poczekalnie. Wdrażając środki zabezpieczeń należy w szczególności uwzględnić:
   a) odpowiednią jakość oświetlenia – co oznacza zapewnienie możliwości identyfikacji poszczególnych osób, zapewnienie światła o właściwym natężeniu tak, aby zapewnić odpowiedni rozkład luminancji, zapobiegając zjawiskom olśnienia i kontrastu;
   b) stan i architekturę zabezpieczeń budowlano-mechanicznych budynków, ścian, drzwi, okien, bram, włazów dachowych;
   c) podniesione krawężniki, ciężkie gazony lub ciągi słupków zabezpieczających lub inne elementy ograniczające, w przypadku gdy wprowadzenie wskazanych zabezpieczeń jest konieczne po oszacowaniu ryzyka.
2. Parkowanie samochodów prywatnych, służbowych na obszarze przynależącym do lokalizacji powinno odbywać się zgodnie z powszechnie obowiązującymi przepisami prawa.
3. Pomieszczenia, w których przetwarzane są informacje powinny być wyposażone w odpowiednie miejsca służące przechowywaniu nośników tych informacji – adekwatne do klasy informacji w nich przechowywanych.

4. Należy sprawować stały nadzór nad punktami dostępu, w szczególności takimi, jak obszary dostaw, wejścia, recepcje oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń (w szczególności znajdujących się w strefie chronionej i administracyjnej). Jeżeli jest to możliwe, wskazane punkty dostępu należy odizolować od miejsc przetwarzania i/lub przechowywania informacji stanowiących tajemnicę Urzędu /informacji wrażliwych lub prawnie chronionych, aby zapobiec nieuprawnionemu dostępowi do wymienionych wyżej informacji.

VIII. Wytyczne dla bezpieczeństwa okablowania strukturalnego

1. Okablowanie zasilające oraz telekomunikacyjne lub wspomagające usługi informacyjne powinno być chronione przed przechwyceniem, nieautoryzowanym wpięciem, zakłóceniem lub uszkodzeniem.
2. W skład systemów okablowania w zakresie konstrukcyjno-mechanicznym wchodzą w szczególności:
   a) trakty kablowe (listwy PCV, szyny, rury, przepusty);
   b) szafy dystrybucyjne;
   c) tablice;
   d) krosownice.
3. Okablowanie powinno być poprowadzone w miejscach bezpiecznych (jeżeli jest to możliwe, linie zasilające oraz telekomunikacyjne powinny być prowadzone pod ziemią), tj. z dala od korytarzy, przejść i ciągów komunikacyjnych. Jeżeli zachodzi konieczność poprowadzenia okablowania w miejscach użyteczności, to muszą być one poprowadzone w rynnach zabezpieczających.
4. Kable powinny być odpowiednio zorganizowane, zapewniając bezpieczeństwo oraz dostępność tj.:
   a) okablowanie prowadzące do tego samego urządzenia powinno być zabezpieczone specjalną tubą osłonową;
   b) grupy kabli biegnących obok siebie powinny być powiązane za pomocą pasków uciskowych (np. w serwerowni);
   c) kable powinny być odpowiednio podwieszone, przy stanowiskach ze sprzętem, w sposób który zapobiega ich prowadzeniu po podłodze.
5. Dla systemów krytycznych należy:
   a) instalować zbrojone rury kablowe i w zamykanych pomieszczeniach lub szafkach w punktach kontrolnych i zakończeń,
   b) korzystać z ekranów elektromagnetycznych w celu ochrony kabli,
   c) kontrolować dostęp do paneli połączeniowych i pomieszczeń z okablowaniem.
6. Wszystkie systemy okablowania powinny podlegać okresowym przeglądom.
7. Należy wyznaczyć osobę/osoby odpowiedzialne za przeprowadzanie przeglądu.
8. Zakres przeglądu powinien w szczególności zawierać:
   a) sprawdzenie stanu technicznego (konstrukcyjno-mechanicznego) elementów systemu okablowania;
   b) sprawdzenie zabezpieczeń elektronicznych dla systemów okablowania polegające na sprawdzeniu poprawności funkcjonowania np. elektronicznych systemów kontroli dostępu zastosowanych do zabezpieczenia szaf dystrybucyjnych, krosownic lub innych urządzeń.
9. Przeglądy powinny zostać przeprowadzane w szczególności poprzez:
   a) sprawdzenie mocowania listew traktów kablowych, w miejscach ogólnie dostępnych, np. narażonych na uszkodzenia mechaniczne, spowodowane przez przenoszenie przedmiotów o dużych gabarytach (biurko, szafa) lub ruch osobowy;
   b) sprawdzenie zamknięcia szaf, tablic, osłon włazów i studzienek zlokalizowanych zarówno wewnątrz jak i poza budynkiem;

c) sprawdzenie czy występują ślady po próbach ingerencji osób nieuprawnionych, itp.;
d) sprawdzenie poszczególnych elementów konstrukcyjno-mechanicznych systemów okablowania powinno opierać się na porównaniu stanu faktycznego (rzeczywistego) z opisem w dokumentacji technicznej;
e) przestrzegania zasad ochrony okablowania oraz punktów połączeń okablowania pod kątem zidentyfikowania podłączonych nieautoryzowanych urządzeń przechwytujących, rejestrujących, transmitujących i zniekształcających sygnał transmisyjny;
f) stanu technicznego instalacji poprzez wykonanie pomiarów okablowania.

10. W przypadku rozbieżności pomiędzy stanem rzeczywistym, a dokumentacją techniczną należy niezwłocznie dokonać aktualizacji dokumentacji technicznej lub przywrócić instalację do stanu opisanego w dokumentacji technicznej.
11. W przypadku stwierdzenia nieautoryzowanej ingerencji w okablowanie lub próby ingerencji poprzez zniszczenie, przechwycenie, wpięcie i inne należy niezwłocznie poinformować właściwe organy śledcze.

IX. Wytyczne bezpieczeństwa dla systemów alarmowych

1. Podmiot zajmujący się instalacją systemów, z chwilą przekazania systemów do eksploatacji, powinien dostarczyć poświadczenie zgodności stwierdzające, że systemy zostały zainstalowane zgodnie z dokumentacją powykonawczą.
2. Po zakończeniu instalacji systemów zabezpieczeń należy je uruchomić i sprawdzić zgodność ze specyfikacją i poziomami funkcjonalności określonymi na etapie projektowania.
3. W przypadku systemów połączonych z Centrum Obsługi / Centrum Nadzoru z wykorzystaniem łącz WiFi (innych bezprzewodowych) należy dbać o wprowadzenie silnych haseł oraz innych zabezpieczeń minimalizujących / uniemożliwiających dostęp do tych urządzeń osobom trzecim.
4. Każde włamanie do elektronicznych systemów bezpieczeństwa fizycznego należy traktować jako incydent krytyczny / bardzo poważny i niezwłocznie informować odpowiednie służby / organy.
5. Po przekazaniu danego systemu do eksploatacji powinien być on poddany testowaniu.
6. Należy wyznaczyć Administratora/Administratorów systemów alarmowych.
7. Administratorzy poszczególnych systemów i – jeżeli to właściwe - ich użytkownicy przed oddaniem systemu do użytkowania powinni uczestniczyć w demonstracji działania danego systemu, łącznie z obsługą urządzeń do sygnalizacji napadu, kontroli dostępu i wizji, z pokazaniem sposobów ich testowania i objaśnieniem procedur komunikacji.
8. Wszystkie systemy powinny zawierać przejrzystą i zwięzłą instrukcję obsługi, zawierającą opis właściwych procedur włączania i wyłączania poszczególnego systemu. Dostęp do instrukcji powinny posiadać wszystkie osoby odpowiedzialne za obsługę danego systemu.
9. Dokumentacja systemów alarmowych powinna zawierać informacje dotyczące:
   a) firmy instalacyjnej: nazwa, adres i numer telefonu firmy bądź dane konkretnego instalatora;
   b) firmy serwisowej odpowiedzialnej za konserwację i naprawy: nazwa, adres i numer telefonu firmy bądź dane osoby odpowiedzialnej za konserwację i/lub naprawy, włącznie ze szczegółową informacją, jak można skontaktować się z tą firmą lub jej dyżurnym przedstawicielem przez całą dobę;
   c) firmy prowadzącej centrum monitoringu: nazwa, adres i numer telefonu centrum monitoringu odpowiedzialnego za reakcję na sygnały alarmowe;

d) zasad weryfikacji przez centrum monitoringu zgłaszanych sygnałów: szczegóły wszelkich procedur związanych z weryfikacją stanu alarmu;
e) firmy podejmującej interwencje: nazwa, adres i numer telefonu organizacji odpowiedzialnej za interwencję w miejscu chronionym w przypadku wystąpienia stanu alarmu.

10. Użytkownikom należy przeprowadzić szkolenia w zakresie obsługi, proporcjonalnie do stopnia złożoności systemów.
11. W przypadku wystąpienia działań niepożądanych należy udokumentować wszystkie działania podjęte wskutek wystąpienia stanów niepożądanych np. alarmów oraz wszelkie naprawy i modyfikacje z tym związane.
12. Należy dokumentować zapisy z systemów – co oznacza, że należy zapisywać:
    a) daty i godziny zgłoszenia stanów alarmowych;
    b) inne dane, np. z którego czujnika doszło do zgłoszenia alarmu.
13. Wszystkie systemy zabezpieczeń podlegają minimum raz na 12 miesięcy (chyba, że producent zaleca częstsze przeglądy) regularnym przeglądom technicznym dokonywanym przez osoby posiadające odpowiednie uprawnienia.
14. Wszystkie systemy zabezpieczeń muszą być systematycznie konserwowane – w tym poddawane przeglądom i serwisowaniu), zaraz po przekazaniu ich do eksploatacji, zgodnie z harmonogramem uzgodnionym z firmą instalacyjną.
15. Przeglądy systemów zabezpieczeń przeprowadzane są każdorazowo w przypadku wystąpienia incydentów zagrażających lub mogących powodować zagrożenie dla bezpieczeństwa osób i mienia.
16. Należy poinformować osoby odpowiedzialne za konserwację systemów zabezpieczeń o ich odpowiedzialności za:
    a) dopuszczenie do obsługi systemów jedynie osób wyszkolonych w tym zakresie oraz zadbanie o to, aby były obsługiwane zgodnie z instrukcjami producentów i po odbyciu stosownych szkoleń;
    b) bezzwłoczne zgłaszanie wszelkich usterek do właściwej firmy serwisowej;
    c) zgłaszanie planów wszelkich zmian aranżacyjnych w poszczególnych strefach bezpieczeństwa lub planowanych zmian w sposobie ich użytkowania.

X. Postępowanie w przypadku zagrożeń

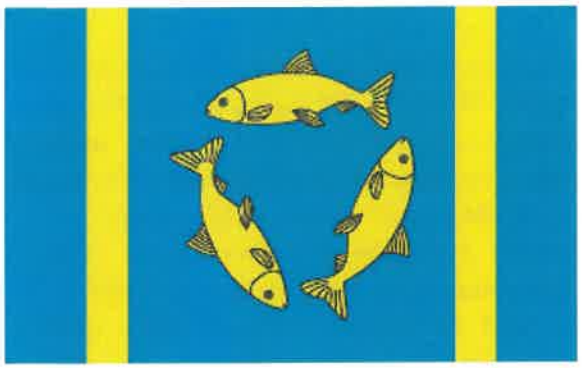
1. W Urzędzie są wprowadzone instrukcje alarmowe na wypadek zagrożenia wraz z niezbędnymi numerami telefonów.
2. Alarmowanie i reagowanie na zagrożenia odbywa się zgodnie z obowiązującymi instrukcjami i procedurami.
3. Minimum raz na 12 miesięcy jest przeprowadzany przegląd instrukcji alarmowych pod kątem aktualności zawartych w nich zapisów ze szczególnym uwzględnieniem weryfikacji aktualności numerów telefonów.
4. Każda osoba przebywająca na terenie Urzędu jest zobowiązana do reagowania na zdarzenie mogące mieć wpływ na bezpieczeństwo budynku, instalacji lub pozostających w nim osób.

XI. Postanowienia końcowe – przeglądy i zmiany zapisów

1. Przegląd niniejszych Procedur jest dokonywany co najmniej raz w roku przez Grupę Roboczą złożoną co najmniej z Koordynatora ds. bezpieczeństwa technicznego, środowiskowego i fizycznego oraz Pełnomocnika ds. BI i CD, a także bezzwłocznie w przypadkach wymagających przeglądu SZBI na podstawie Załącznika nr 4 do ustawy o KSC.
2. W przypadku zmiany przepisów lub istotnej zmiany kontekstu działania należy niezwłocznie dokonać przeglądu niniejszych Procedurach oraz jeżeli istnieje taka potrzeba dokonać ich aktualizacji.

3. Każda zmiana Procedur oraz realizacja istotnych działań wynikających z przeglądu, testów, incydentów lub szacowania ryzyka musi zostać udokumentowana.





DOKUMENT SYSTEMU ZARZĄDZANIA

BEZPIECZEŃSTWEM INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

Zasady bezpieczeństwa informacji w relacjach z dostawcami

Nazwa dokumentu	**Zasady bezpieczeństwa informacji w relacjach z dostawcami**
Autor dokumentu	Joanna Mrowicka
Sprawdzająca dokument	Aneta Skrzypczak-Kurzawa
Wersja dokumentu	0.2
Zatwierdzający dokument	Wójt Gminy
Data zatwierdzenia dokumentu	15 września 2026r.

I. Cel i zakres dokumentu

1. **Zasady bezpieczeństwa w zarządzaniu dostawcami mają na celu ochronę aktywów informacyjnych Urzędu Gminy Chrzypsko Wielkie, zwanego dalej Urzędem Gminy lub Urzędem, udostępnianych stronom trzecim czyli dostawcom i osobom z zewnątrz oraz utrzymanie uzgodnionego poziomu bezpieczeństwa informacji, ciągłości działania i świadczonych usług zgodnie z umowami z dostawcami.**
2. Zasady bezpieczeństwa informacji w relacjach z dostawcami wynikają z Polityki Bezpieczeństwa Informacji i Ciągłości Działania oraz wspierają realizację SZBI wymaganego w art. 8 ust. 3 i Załączniku nr 4 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20, 252, 815, z późn. zm.). W szczególności mają zapewnić udokumentowanie mechanizmów ochrony przy korzystaniu z chmury obliczeniowej i centrów przetwarzania danych oraz odpowiedni poziom bezpieczeństwa umów serwisowych.
3. Zasady stosuje się do dostawców mających dostęp do informacji, produktów ICT, usług ICT lub procesów ICT Urzędu. W przypadku wspólnych zamówień lub wspólnej obsługi cyberbezpieczeństwa obejmującej jednostki organizacyjne Gminy, wymagania bezpieczeństwa należy stosować spójnie w odniesieniu do wszystkich jednostek objętych daną usługą, z poszanowaniem odpowiedzialności ich kierowników.

II. Postanowienie ogólne

1. Zapewnia się, że dostawca jest świadomy swoich zobowiązań i akceptuje odpowiedzialność związaną z przyznawanym dostępem do aktywów należących do Urzędu Gminy i zapoznał się, jeśli jest to wymagane, z całością lub istotną częścią Polityki Bezpieczeństwa Informacji i Ciągłości Działania oraz innymi dokumentami uzupełniającymi lub wspierającymi i powiązanymi.
2. Pracownik Urzędu współpracując z dostawcą jest zobowiązany zapewnić bezpieczeństwo przetwarzanych informacji przy pomocy zabezpieczeń prawnych i technicznych (w tym teleinformatycznych), w sposób uniemożliwiający dostęp do tych informacji osobom nieuprawnionym.
3. Osoby reprezentujące dostawcę odpowiadają za zapoznanie się z zasadami bezpieczeństwa w związku z dostępem do informacji chronionych w Urzędzie.

III. Stosowanie zabezpieczeń oraz zasad postępowania z informacjami w relacjach z dostawcami

1. Udostępnienie aktywów informacyjnych Urzędu dostawcy jest dopuszczalne wyłącznie na podstawie odpowiedniej podstawy prawnej i umowy określającej wymagania bezpieczeństwa. Przed zawarciem umowy przeprowadza się udokumentowaną ocenę dostawcy adekwatną do ryzyka, obejmującą co najmniej ochronę danych osobowych, bezpieczeństwo informacji, ciągłość działania, sposób reagowania na incydenty, zarządzanie podatnościami i podwykonawcami. Certyfikat zgodności, w tym ISO/IEC 27001, może stanowić dowód pomocniczy, lecz nie zwalnia automatycznie z oceny dostawcy i warunków konkretnej usługi.
2. Umowa powinna wymuszać stosowanie zabezpieczeń adekwatnych do poziomu klasyfikacji informacji.
3. Umowa dotycząca współpracy z dostawcą powinna zawierać zabezpieczenia i klauzule poufności adekwatne do zakresu dostępu, mechanizmy weryfikacji ich stosowania oraz wymagania dotyczące zgłaszania incydentów i podatności. Jeżeli dostawca świadczy usługę chmury obliczeniowej albo usługę centrum przetwarzania danych, przed uruchomieniem usługi należy udokumentować mechanizmy ochrony informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniem i zakłóceniami.
4. Właściciel merytoryczny umowy, przed zawarciem lub istotną zmianą umowy, przeprowadza i dokumentuje analizę ryzyka związanego z dostępem dostawcy do aktywów informacyjnych. Analiza uwzględnia w szczególności:
   a) poziom bezpieczeństwa informacji, do których dostawca ma uzyskać dostęp;

b) środki przetwarzania informacji;
c) sposób dostępu do informacji.
d) krytyczność usługi i jej wpływ na realizację zadań publicznych oraz ciągłość działania;
e) znane podatności, cykl życia i warunki aktualizacji produktów ICT lub usług ICT wykorzystywanych przez dostawcę;
f) lokalizację przetwarzania, model usługi chmurowej lub centrum danych, sposób wykonywania i odtwarzania kopii zapasowych;
g) wykorzystanie podwykonawców oraz zależności w łańcuchu dostaw;
h) mechanizmy wykrywania i zgłaszania incydentów, czasy reakcji, SLA oraz zasady współpracy z Urzędem i właściwymi CSIRT.

5. Udostępniając dostawcy informacje należy:
   a) przekazywać tylko te informacje, które są niezbędne do wykonywania powierzonej pracy;
   b) przed przekazaniem informacji, w sposób wyraźny i niebudzący wątpliwości, zastrzec poufność przekazywanych informacji.
6. Zabrania się pozostawiania bez nadzoru przedstawicieli dostawców, realizujących prace serwisowe lub wdrożeniowe na środkach przetwarzających informacje chronione w Urzędzie. Prace te muszą odbywać się pod nadzorem pracowników Urzędzie Gminy. W przypadku dostępu zdalnego do zasobów teleinformatycznych stosuje się zasady zarządzania systemami informatycznymi.
7. Zobowiązuje się dostawcę, aby informacje uzyskane podczas realizacji umów z Urzędem Gminy nie były wykorzystane w celach marketingowych.
8. Przy przetwarzaniu informacji chronionych w systemach informatycznych przez dostawców, należy zawrzeć w umowie postanowienia regulujące sposób postępowania z informacjami zgodnie z zasadami opisanymi w RODO.

IV. Wykaz zabezpieczeń stosowanych w umowach z dostawcami

1. Przy przygotowywaniu projektu umowy należy, adekwatnie do wyniku analizy ryzyka i charakteru usługi, uwzględnić następujące postanowienia bezpieczeństwa:
   a) zabezpieczeń uwzględniających wymagania wynikające z odrębnych przepisów;
   b) zabezpieczeń chroniących aktywa;
   c) mechanizmy ochrony fizycznej;
   d) zabezpieczenia chroniące przed złośliwym oprogramowaniem;
   e) procedury dotyczące utraty lub modyfikacji danych, oprogramowania lub sprzętu;
   f) zabezpieczenia zapewniające zwrot aktywów w chwili zakończenia realizacji umowy w określonym czasie;
   g) ograniczenia w zakresie kopiowania informacji;
   h) szkoleń osób z zewnątrz w zakresie bezpieczeństwa informacji;
   i) przypisania użytkownikom odpowiedzialności za bezpieczeństwo informacji;
   j) odpowiedzialności związanej z instalowaniem i utrzymywaniem oprogramowania i sprzętu, zdefiniowania kryteriów wydajności oraz monitorowania;
   k) zasad raportowania, opracowania formularzy;
   l) zasad oraz procedury kontroli dostępu;
   m) zasad postępowania ze zidentyfikowanymi problemami lub incydentami oraz zasad postępowania w celu ich rozwiązania;
   n) zapewnienia prawa do monitorowania wszelkich działań związanych z aktywami Urzędu;
   o) zapewnienie prawa do przeprowadzenia audytów u dostawcy;
   p) wymagań dotyczących ciągłości działania;
   q) określenia oczekiwanego poziomu usług (SLA);

r) zasad współpracy dostawcy z podwykonawcami oraz zabezpieczeń, jakie podwykonawcy mają wdrożyć z uwzględnieniem zasad odpowiedzialności w przypadku zaangażowania podwykonawców;
s) zasad dotyczących renegocjacji lub zakończenia umowy;
t) zasad dotyczących kar za niewywiązanie się dostawcy z warunków umowy;
u) zasad dotyczących wymiany informacji.
v) obowiązku niezwłocznego informowania Urzędu o incydencie, cyberzagrożeniu lub podatności mogących mieć wpływ na dane, systemy lub zadania publiczne Urzędu, wraz z obowiązkiem współpracy przy obsłudze incydentu;
w) zasad zarządzania podatnościami, aktualizacjami i cyklem życia wykorzystywanego oprogramowania i sprzętu, w tym terminów usuwania podatności krytycznych;
x) wymagań dotyczących kopii zapasowych, testów odtworzeniowych oraz odseparowania kopii, jeżeli dostawca odpowiada za ich wykonywanie;
y) zasad zakończenia usługi, zwrotu lub bezpiecznego usunięcia danych i aktywów, przeniesienia usług oraz zapewnienia ciągłości w okresie wyjścia z umowy;
z) w przypadku chmury obliczeniowej lub centrum przetwarzania danych - obowiązku przedstawienia i aktualizowania opisu mechanizmów ochrony fizycznej, technicznej i organizacyjnej.

2. W przypadku powierzenia dostawcy prac rozwojowych nad oprogramowaniem należy dokonać ustaleń dotyczących licencji, własności kodu źródłowego, prawa do własności intelektualnej oraz praw autorskich majątkowych.

V. Procedura zarządzania usługami świadczonymi przez dostawców

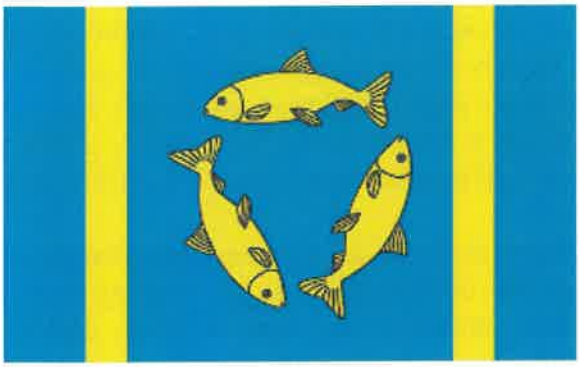
1. Kontrolę nad działalnością dostawcy i bieżące monitorowanie stanu podpisanych umów przeprowadzają właściciele merytoryczni umów wyznaczeni po stronie Urzędu.
2. Właściciel merytoryczny umowy co najmniej raz w roku oraz po istotnym incydencie, zmianie zakresu usługi, zmianie podwykonawcy, ujawnieniu krytycznej podatności albo istotnej zmianie technologii dokonuje udokumentowanej oceny współpracy z dostawcą pod kątem bezpieczeństwa informacji, ochrony danych osobowych, ciągłości działania, spełniania wymagań umownych i KSC oraz skuteczności działań naprawczych.
3. W przypadku zmiany warunków wykonywania usługi lub czynników zewnętrznych mogących wpłynąć na ryzyko, w tym rekomendacji właściwych organów lub informacji o istotnych podatnościach, należy ponownie ocenić ryzyko i - w razie potrzeby - zmienić wymagania bezpieczeństwa albo wdrożyć dodatkowe zabezpieczenia.
4. Umowa zawarta z dostawcą oraz przepisy prawa określają odpowiedzialność za:
   a) ujawnienie osobom nieuprawnionym informacji dotyczących Urzędu i będących jego własnością;
   b) umożliwienie osobom nieuprawnionym dostępu do informacji i zasobów informatycznych będących własnością Urzędu które zostały udostępnione osobie reprezentującej dostawcę w czasie przeprowadzania niezbędnych prac wynikających z umowy;
   c) umożliwienie osobom trzecim, nieupoważnionym dostęp do stref chronionych / zamkniętych;
   d) kradzież, w tym kradzież informacji;
   e) spowodowanie zagrożenia bezpieczeństwa zasobów teleinformatycznych Urzędu.
5. Nieprzestrzeganie powyższych zasad może stanowić podstawę:
   a) rozwiązania umowy z dostawcą;
   b) wystąpienia o naprawienie szkody wyrządzonej na skutek naruszenia przedmiotowych zasad;

c) zastosowania innych, odpowiednich wobec skali dokonanego naruszenia, środków prawnych, w tym poinformowanie organów ścigania czy złożenie zawiadomienia do Prokuratury / wystąpienie na drogę sądową.

VI. Przeglądy oraz aktualizacja Procedury

1. Przegląd niniejszych Zasad jest dokonywany co najmniej raz w roku przez Komitet Bezpieczeństwa oraz bezzwłocznie w przypadkach powodujących konieczność przeglądu SZBI zgodnie z Załącznikiem nr 4 do ustawy o KSC.
2. W przypadku zmiany przepisów lub istotnej zmiany kontekstu działania należy niezwłocznie dokonać przeglądu niniejszej Procedury oraz jeżeli istnieje taka potrzeba dokonać jej aktualizacji.
3. Za aktualizację niniejszej Procedury odpowiada wyznaczona przez Wójta osoba w koordynacji z Pełnomocnikiem ds. BI i CD.
4. Każda zmiana Zasad oraz istotne wyniki oceny dostawców i realizacji działań bezpieczeństwa muszą zostać udokumentowane.

Wójt
mgr inż. Edmund Ziółek



DOKUMENT SYSTEMU ZARZĄDZANIA

BEZPIECZEŃSTWEM INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

Zasady klasyfikacji informacji i postępowania z informacjami

Nazwa dokumentu	**Zasady klasyfikacji in formacji i postepowania z informacjami**
Autor dokumentu	Joanna Mrowicka
Sprawdzająca dokument	Aneta Skrzypczak-Kurzawa
Wersja dokumentu	0.2
Zatwierdzający dokument	Wójt Gminy
Data zatwierdzenia dokumentu	15 września 2026r.

I. Cel i zakres dokumentu

1. Celem opracowania i wprowadzenia niniejszych Zasad jest zdefiniowanie jednolitych standardów klasyfikacji i postępowania z informacjami w Urzędzie Gminy Chrzypsko Wielkie, wspierających wymagania ochrony informacji, kontroli dostępu i minimalnych uprawnień określone w Załączniku nr 4 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20, 252, 815, z późn. zm.).
2. Dokument obowiązuje we wszystkich lokalizacjach i komórkach organizacyjnych Urzędu, obowiązuje cały personel Urzędu oraz obowiązuje podczas wymiany danych z podmiotami zewnętrznymi (trzecimi) oraz ramach wewnętrznej wymiany danych.
3. W jednostkach organizacyjnych Gminy niniejsze Zasady stosuje się po ich formalnym wprowadzeniu w danej jednostce albo w zakresie objętym wspólną obsługą cyberbezpieczeństwa. Kierownik każdej jednostki pozostaje odpowiedzialny za zapewnienie zgodności postępowania z informacjami z przepisami właściwymi dla tej jednostki.

II. Role – odpowiedzialność

1. Kierownik jednostki na podstawie osobnego dokumentu wyznaczy osobę/osoby, którym deleguje uprawnienia do upubliczniania dokumentów.
2. Osoby upoważnione do upubliczniania dokumentu będą wymienione z imienia i nazwiska oraz stanowiska pełnionego w Urzędzie.
3. Lista osób z uprawnieniami (Rejestr upoważnień) będzie aktualizowana przynajmniej raz na 12 miesięcy lub w przypadku zmiany roli i obowiązków, którejś z uprawnionych osób, a także rozwiązania stosunku pracy lub umowy cywilno-prawnej.

III. Zasady klasyfikacji informacji

1. W Urzędzie przyjęto następujące klasy informacji:
   - 1.1 **Informacje publiczne** – stanowią wszelkie informacje:
     a) publiczne wykorzystywane przez Urząd pozyskane od innych podmiotów;
     b) co do których upubliczniania Urząd jest zobowiązany przepisami prawa;
     c) dla których podjęta została decyzja o ich upublicznieniu przez Wójta Gminy lub osobę upoważnioną do reprezentowania Urzędu na zewnątrz w zakresie swoich zadań służbowych.
   - 1.2 **Informacje wewnętrzne** – informacje wykorzystywane w bieżącej pracy Urzędu, które nie zaliczają się do informacji chronionych i nie podjęto dla nich decyzji o upublicznieniu.
   - 1.3 **Informacje chronione** – obejmujące wszelkie informacje podlegające ochronie określonej przepisami prawa, w tym: dane osobowe i informacje stanowiące tajemnicę przedsiębiorstwa oraz wszelkie informacje pozyskane od klientów i kontrahentów, co do których zaznaczyli oni, że stanowią one tajemnicę. Kierownik jednostki może wskazać listę informacji objętych tajemnicą przedsiębiorstwa lub stanowiących tajemnicę Urzędu (z wyłączeniem informacji niejawnych, do których mają zastosowania przepisy Ustawy o ochronie informacji niejawnych).

IV. Podstawowe zasady postępowania z informacjami

1. Wójt na podstawie osobnych dokumentów ustali wzór oznakowania dokumentów publicznych, wewnętrznych i chronionych oraz zasady ich znakowania.
2. Wszystkie informacje, dane i dokumenty klasyfikuje się z uwzględnieniem wymaganej poufności, integralności, dostępności i autentyczności oraz ich wartości dla Urzędu. Klasyfikacja służy do doboru zabezpieczeń, w tym kontroli dostępu, sposobu przesyłania, przechowywania, wykonywania kopii zapasowych i niszczenia.

3. Za nadanie sklasyfikowania informacji, zgodnie z przyjętym modelem odpowiada wytwórca tej informacji lub osoba, która ją otrzymała.
4. Informacje zawarte w dokumentacji kadrowo-płacowej są zawsze określane jako informacje chronione.
5. Dokumenty, które nie są wyraźnie opisane jako informacje publiczne powinny być traktowane jako informacje wewnętrzne.
6. Dokumenty powinny być opisane tak, aby wszyscy ich użytkownicy byli świadomi, kto jest właścicielem dokumentu i jak jest klasyfikacja dokumentu.
7. Wszystkie informacje, dane i dokumenty muszą być przetwarzane i przechowywane zgodnie z poziomem klasyfikacji przypisanym do informacji w nich zawartych (przypisuje się najwyższy poziom ochrony).
8. Nadanie informacji klasy „Informacja publiczna" wymaga zgody Wójta lub przez niego osoby upoważnionej.
9. Wszystkie informacje lub dokumenty, nośniki nieoznaczone jako „Publiczne" należy traktować co najmniej jako „Informacje wewnętrzne".
10. Zmiany klasyfikacji informacji może dokonać:
    a) Osoba odpowiedzialna za pracę danej komórki organizacyjnej, w której informacja została wytworzona lub przez którą informacja została otrzymana;
    b) Kierownik Urzędu;
    c) Osoba upoważniona w tym zakresie przez Wójta w oparciu o oddzielny dokument.
11. W przypadku wątpliwości co do klasyfikacji informacji należy skontaktować się z Pełnomocnikiem ds. BI i CD lub Inspektorem Ochrony Danych (w zakresie informacji dotyczących ochrony danych osobowych).
12. Dostęp do informacji, niezależnie od klasy, przyznaje się wyłącznie w zakresie niezbędnym do wykonywania zadań. Uprawnienia są modyfikowane przy zmianie zadań, bezzwłocznie cofane po ustaniu podstawy dostępu oraz zawieszane w przypadkach przewidzianych w SZBI.
13. Przy udostępnianiu informacji podmiotom zewnętrznym należy zweryfikować tożsamość i uprawnienie odbiorcy, zakres niezbędnych informacji oraz właściwy kanał przekazania; zasady te stosuje się także do pracy zdalnej, urządzeń mobilnych i usług chmurowych.

V. Wymagania bezpieczeństwa dla poszczególnych klas informacji

1. Informacje publiczne:

1.1 Oznaczanie: zalecane oznaczenie jako „informacja publiczna".

1.2 Przesyłanie/przenoszenie: brak wymagań poufności wynikających wyłącznie z klasy „publiczna"; należy jednak zapewnić integralność i autentyczność informacji oraz stosować zatwierdzone kanały publikacji i komunikacji.

1.3 Przechowywanie: w sposób zapewniający integralność, dostępność i ochronę przed nieuprawnioną zmianą; wersje elektroniczne podlegają zasadom zarządzania uprawnieniami, kopiami zapasowymi i aktualnością systemów.

1.4 Niszczenie: brak wymagań.

2. Informacje wewnętrzne

2.1 Oznaczenie: zalecane oznaczenie jako „informacja wewnętrzna".

2.2 Przesyłanie/przenoszenie: tylko w ramach wewnętrznej sieci lub korespondencji oraz w ramach komunikacji zewnętrznej jeżeli wymagają tego umowy z dokładnym sprecyzowaniem klasyfikacji informacji.

2.3 Przechowywanie: kontenery/szafki do przechowywania informacji (wersja papierowa), wersja elektroniczna zgodnie z procedurami IT.

2.4 Niszczenie: nośniki informacji niszczone fizycznie (np. dokumenty papierowe w niszczarce).

3. **Informacje chronione:**

3.1 Oznaczanie: zalecane oznaczenie jako „informacja chroniona", szczególnie w przypadkach kiedy nie są to typowe dokumenty wykorzystywane w Urzędzie. W komunikacji zewnętrznej zalecane jest sprecyzowanie rodzaju informacji chronionej (np. dane osobowe, tajemnica przedsiębiorstwa itp.).

3.2 Przesyłanie/przenoszenie:

- Forma tradycyjna (dokument papierowy, płyta CD):
  a. Wewnątrz Urzędu: pod nadzorem pracownika/ współpracownika.
  b. Poza Urząd: w zaklejonej kopercie, z weryfikacją adresata (np. list polecony), do rąk własnych.
- Forma elektroniczna:
  a. Wewnątrz Urzędu: wymagana weryfikacja adresata.
  b. Poza Urząd: informacje chronione przesyła się z wykorzystaniem zatwierdzonych mechanizmów szyfrowania lub innego bezpiecznego kanału komunikacji adekwatnego do ryzyka. Jeżeli stosowane jest hasło lub klucz przekazywany odbiorcy, należy przekazać go odrębnym kanałem komunikacji.

3.3 Przechowywanie:

- Forma tradycyjna (dokument papierowy, płyta CD) – zamknięta szafka lub zamykane pomieszczenie bez dostępu osób postronnych.
- Forma elektroniczna:
  a. Urządzenie mobilne/nośnik: wymagane jest szyfrowanie danych lub nośnika z wykorzystaniem zatwierdzonego mechanizmu kryptograficznego, kontrola dostępu, możliwość zablokowania lub odebrania dostępu oraz stosowanie zasad bezpiecznej pracy mobilnej i zdalnej.
  b. Serwer/komputer stacjonarny: dostęp wyłącznie dla osób uprawnionych zgodnie z zasadą minimalnych uprawnień; obowiązują mechanizmy uwierzytelniania, ochrona antymalware, aktualizacje, kopie zapasowe i inne zabezpieczenia przewidziane w SZBI. Szyfrowanie stosuje się, gdy wynika to z analizy ryzyka, wymagań prawnych lub architektury systemu.

3.4 Niszczenie:

- Nośniki informacji niszczone fizycznie (np. dokumenty papierowe w niszczarce). Przygotowany „Protokół z niszczenia nośników informacji" przez osobę, która dokonała zniszczenia nośnika informacji.
- Osoba dokonująca zniszczenia nośników informacji zobowiązana jest przygotować „Protokół z niszczenia nośników informacji".

VI. Przegląd oraz aktualizacja Zasad

1. Przegląd niniejszego dokumentu jest dokonywany co najmniej raz w roku przez Pełnomocnika ds. BI i CD w koordynacji z IOD.
2. Przeglądu i aktualizacji Zasad można dokonać w ramach obrad Komitetu Bezpieczeństwa w czasie prac warsztatowych nad aktualizacją Polityki Bezpieczeństwa i dokumentów powiązanych.
3. Przegląd jest wykonywany bezzwłocznie także po zmianie przepisów, po rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa dotyczącej systemów lub usług ICT Urzędu oraz w razie wystąpienia okoliczności mogących wpłynąć na ryzyko incydentu poważnego.
4. Każda zmiana Zasad oraz istotne działania wynikające z ich stosowania i przeglądu muszą zostać udokumentowane.

Wójt
mgr inż. Edmund Ziółek