ZARZĄDZENIE NR 154/21

Burmistrza Gminy Żychlin

z dnia 21 grudnia 2021r.

w sprawie wprowadzenia w Urzędzie Gminy w Żychlinie Systemu Zarządzania Bezpieczeństwem Informacji.

Na podstawie art. 33 ust. 3 i 5 z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2021 r. poz. 1372 z późn. zm.) zarządza się, co następuje:

§ 1. Wprowadza się do stosowania w Urzędzie Gminy w Żychlinie System Zarządzania Bezpieczeństwem Informacji (SZBI) składający się z następujących polityk oraz procedur:

1) Polityka Bezpieczeństwa Informacji,
2) Polityka w zakresie organizacji wewnętrznej,
3) Polityka stosowania urządzeń mobilnych i telepracy,
4) Polityka bezpieczeństwa zasobów ludzkich,
5) Polityka zarządzania aktywami,
6) Polityka kontroli dostępu,
7) Polityka stosowania zabezpieczeń kryptograficznych,
8) Polityka bezpieczeństwa fizycznego i środowiskowego,
9) Polityka bezpiecznej eksploatacji,
10) Polityka bezpieczeństwa komunikacji,
11) Polityka pozyskiwania, rozwoju i utrzymania systemów,
12) Polityka relacji z dostawcami,
13) Polityka zarządzania incydentami,
14) Polityka zarządzania ciągłością działania,
15) Polityka zapewnienia zgodności,
16) Polityka oceny i zarządzania ryzykiem,
17) Procedury bezpieczeństwa fizycznego i środowiskowego w zakresie ochrony fizycznej budynków i pomieszczeń, postępowania z kluczami i kopiami zapasowymi kluczy,
18) Plan ciągłości działania w zakresie dysfunkcji kluczowych systemów informacyjnych,
19) Procedury postępowania w przypadku incydentów bezpieczeństwa informacji oraz stwierdzonych niezgodności lub naruszeń,

20) Procedury zarządzania systemami informacyjnymi.

stanowiących załączniki do niniejszego Zarządzenia.

§ 2. 1. Funkcję Administratora Systemów Informatycznych (ASI), o której mowa w politykach i procedurach Systemu Zarządzania Bezpieczeństwem Informacji pełni Pan Konrad Melcher.

2. Funkcję Pełnomocnika ds. Systemu Zarządzania Bezpieczeństwem Informacji (Pełnomocnik ds. SZBI) oraz Inspektora Ochrony Danych (IOD), o której mowa w politykach i procedurach Systemu Zarządzania Bezpieczeństwem Informacji pełni Pan Maciej Strycharz.

§ 3. Zobowiązuje się pracowników Urzędu Gminy w Żychlinie do zapoznania się z politykami i procedurami w zakresie wyznaczonym przez Sekretarza.

§ 4. W celu realizacji wymogów bezpieczeństwa podaniu do publicznej wiadomości podlega wyłącznie Polityka Bezpieczeństwa Informacji wraz z Deklaracją Stosowania, stanowiące załącznik nr 1 do niniejszego zarządzenia.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

§ 6. Wykonanie zarządzenia powierza się Sekretarzowi, Administratorowi Systemów Informatycznych i Pełnomocnikowi ds. Systemu Zarządzania Bezpieczeństwem Informacji.

§ 7. Tracą moc zarządzenie nr 48 /2018 Burmistrza Gminy Żychlin z dnia 25 maja 2018 roku w sprawie wprowadzenia do stosowania Dokumentacji Ochrony Danych Osobowych Urzędu Gminy w Żychlinie oraz Zarządzenie nr 110/18 Burmistrza Gminy Żychlin z dnia 26 października 2018 roku w sprawie przyjęcia metodologii szacowania ryzyka dla zasobów danych osobowych w Urzędzie Gminy w Żychlinie.

BURMISTRZ

Grzegorz Ambroziak

Załączniki:

1. Polityka Bezpieczeństwa Informacji,
2. Polityka w zakresie organizacji wewnętrznej,
3. Polityka stosowania urządzeń mobilnych i telepracy,
4. Polityka bezpieczeństwa zasobów ludzkich,
5. Polityka zarządzania aktywami,
6. Polityka kontroli dostępu,
7. Polityka stosowania zabezpieczeń kryptograficznych,
8. Polityka bezpieczeństwa fizycznego i środowiskowego,
9. Polityka bezpiecznej eksploatacji,

10. Polityka bezpieczeństwa komunikacji,
11. Polityka pozyskiwania, rozwoju i utrzymania systemów,
12. Polityka relacji z dostawcami,
13. Polityka zarządzania incydentami,
14. Polityka zarządzania ciągłością działania,
15. Polityka zapewnienia zgodności,
16. Polityka oceny i zarządzania ryzykiem.
17. Procedury bezpieczeństwa fizycznego i środowiskowego w zakresie ochrony fizycznej budynków i pomieszczeń, postępowania z kluczami i kopiami zapasowymi kluczy,
18. Plan ciągłości działania w zakresie dysfunkcji kluczowych systemów informacyjnych,
19. Procedury postępowania w przypadku incydentów bezpieczeństwa informacji oraz stwierdzonych niezgodności lub naruszeń.
20. Procedury zarządzania systemami informacyjnymi.

Załącznik nr 1 do
Zarządzenia Nr 154/21
Burmistrza Gminy Żychlin
z dnia 21 grudnia 2021r.

System Zarządzania Bezpieczeństwem Informacji (SZBI)		
Urząd Gminy w Żychlinie	Dokument SZBI	Data zgodna z Zarządzeniem
P-00	Polityka Bezpieczeństwa Informacji	Strona 1 z 29

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Spis treści

I. Wprowadzenie i zakres

§ 1. 1. Zakres Systemu Bezpieczeństwa Informacji (SZBI) obejmuje Urząd Gminy w Żychlinie.

2. Niniejsza Polityka bezpieczeństwa informacji (PBI) określa wymagania dotyczące ustanawiania, wdrażania, monitorowania, przeglądu, utrzymywania i doskonalenia udokumentowanego SZBI w kontekście ogólnych wymagań Urzędu. Określa on wdrożenie kontroli bezpieczeństwa dostosowanych do potrzeb Urzędu.

3. Niniejsza polityka dotyczy wszystkich pracowników Urzędu, jak również uprawnionych dostawców przez których uznaje się osoby wymienione § 4.

§ 2. 1. Celem SZBI jest zapewnienie odpowiednich i właściwych środków kontroli bezpieczeństwa, które utrzymują poufność, integralność i dostępność informacji.

2. Odnośnie do możliwości zastosowania i wyłączenia (z uzasadnieniem) środków kontroli bezpieczeństwa należy odnieść się do Deklaracji Stosowania (DS) opisanej w załączniku nr 1 do PBI.

II. Powołania normatywne

§ 3. SZBI został opracowany w oparciu o wymogi lub z uwzględnieniem:

1) normy PN-EN ISO/IEC 27001:2017-06,
2) rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zmianą ogłoszoną w Dz. Urz. UE L 127 z 23.05.2018, str. 2),
3) rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,
4) ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach,
5) ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych,
6) ustawy z dnia 29 września 1994 r. o rachunkowości,

7) ustawy z dnia 6 czerwca 1997 r. - Kodeks karny – Rozdział XXXIII Przestępstwa przeciwko ochronie informacji,
8) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej,
9) ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
10) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,
11) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
12) ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

III. Terminy i definicje

§ 4. Zastosowane w SZBI pojęcia oznaczają:

1) **Administrator systemów informacyjnych (ASI)** – osoba odpowiedzialna, w granicach określonych zakresem obowiązków pracowniczych, poleceniami służbowymi i SZBI, za zapewnienie bezpieczeństwa informacji oraz systemów informacyjnych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są informacje oraz za podejmowanie odpowiednich działań w przypadku zidentyfikowania incydentów lub zdarzeń związanych z bezpieczeństwem informacji.
2) **Aktywa** – wszystko, co ma wartość dla Urzędu.
3) **Aktywa informacyjne (informacje lub zasoby informacyjne)** – wszelkie informacje, które mają wartość dla Urzędu, których nieuprawnione ujawnienie, modyfikacja, utrata, uszkodzenie lub zniszczenie itp., spowodowałoby lub mogłoby spowodować szkody dla Urzędu lub interesariuszy albo byłoby z punktu widzenia interesów Urzędu lub interesariuszy niekorzystne, takie jak: dane osobowe, informacje niejawne, dane objęte tajemnicą zawodową, skarbową, handlową, bankową, pracodawcy, przedsiębiorstwa, dane finansowe, podatkowe itp.
4) **Ocena ryzyka** – proces szacowania ryzyka bezpieczeństwa informacji określony w Polityce oceny i zarządzania ryzykiem będącej częścią SZBI.
5) **Bezpieczeństwo informacji** – zapewnienie poufności, integralności i dostępności informacji.
6) **Burmistrz** – Burmistrz Gminy Żychlin,

7) **Cel kontroli** – deklaracja intencji w odniesieniu do danej dziedziny w zakresie niektórych aspektów zasobów lub procesów Urzędu. W odniesieniu do SZBI stanowią one ramy dla opracowania strategii spełnienia zestawu wymagań bezpieczeństwa.
8) **Ciągłe doskonalenie** – stopniowe dążenie do maksymalnego poziomu bezpieczeństwa informacji w Urzędu.
9) **Deklaracja stosowania (DS)** – lista celów bezpieczeństwa informacji i zastosowanych zabezpieczeń (załącznik nr 1 do PBI).
10) **Dokument systemu (systemowy)** – polityka stanowiąca składową dokumentów (dokumentacji) SZBI, ogłoszona zarządzeniem Burmistrza.
11) **Dokument wykonawczy** – dokument (procedura), w tym powiązany z nim formularz (załącznik) opracowany na podstawie dokumentu systemu w celu jego realizacji, zatwierdzony przez Burmistrza lub jakikolwiek dowód procesu, zasady, działania czy postępowania.
12) **Dokumentacja SZBI** – dokumenty systemu i wykonawcze oraz powiązane z nimi formularze (załączniki), które obowiązują pracowników i uprawnionych dostawców.
13) **Dokumentowanie (udokumentowanie)** – uzyskanie jakichkolwiek dowodów potwierdzających realizację postanowień dokumentów systemu (systemowych) np. dokument wykonawczy.
14) **Dostawca** – podmiot zewnętrzny dostarczający produkty lub usługi.
15) **Dostępność** – właściwość zasoby określająca, że jest on możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do dostępu do zasobu.
16) **Incydent (incydent związany z bezpieczeństwem informacji)** – niepożądane lub niespodziewane zdarzenie, które może z dużym prawdopodobieństwem negatywnie wpłynąć na działalność stwarzając zagrożenie dla bezpieczeństwa informacji.
17) **Integralność** – właściwość polegająca na tym, że dany zasób nie został zmodyfikowany w sposób nieuprawniony.
18) **Interesariusze** – grupy bądź osoby zainteresowane działalnością Urzędu i wysuwające wobec niego żądania, podmioty wpływające na poziom ryzyka bezpieczeństwa informacji w urzędzie, podmioty pozostające w przymusowym lub dobrowolnym związku z Urzędem, itp.

19) **Kontrola (mechanizmy kontrolne)** – procedury wdrożone w celu przeglądu SZBI i postępowania z ryzykiem.
20) **Najwyższe kierownictwo** – Burmistrz, Zastępca Burmistrza, Sekretarz.
21) **Nośniki** – wszystkie urządzenia, które mogą przechowywać informacje w formie elektronicznej. Obejmuje to m.in., tablety, smartfony, taśmy, przenośne dyski twarde lub inne urządzenia pamięci masowej (płyty CD/DVD, pendrive'y, karty SD).
22) **Odtwarzanie awaryjne** – plan wczesnego odzyskiwania funkcjonalności w przypadku incydentu, który uniemożliwia normalne działanie Urzędu.
23) **Opiekunowie aktywów (depozytariusze aktywów)** – pracownicy wskazani w dokumencie wykonawczym lub powiązanym z nim formularzu (załączniku).
24) **Urząd** – Urząd Gminy w Żychlinie, ul. Norberta Barlickiego, 99-320 Żychlin.
25) **Plan ciągłości działania (PCD)** – plan mający na celu wbudowanie odpowiedniej nadmiarowości i uniknięcie sytuacji awaryjnych w celu zapewnienia ciągłości działania.
26) **Pracownicy** – osoby zatrudnione przez Urząd zarówno na podstawie umowy o pracę, jak i w oparciu o umowy cywilnoprawne, w tym praktykanci, stażyści, wolontariusze itp. mający dostęp do aktywów i aktywów informacyjnych.
27) **Poufność** – właściwość zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom.
28) **System informacyjny** – system informatyczny, aplikacje lub programy służące lub wykorzystywane do przetwarzania informacji.
29) **System Zarządzania Bezpieczeństwem Informacji (SZBI)** – Ta część ogólnego systemu zarządzania opartego na podejściu do ryzyka, która ma na celu ustanowienie, wdrożenie, obsługę, monitorowanie, przegląd, utrzymanie i poprawę bezpieczeństwa informacji. System zarządzania obejmuje strukturę organizacyjną, zasady, działania planistyczne, obowiązki, praktyki, procedury, procesy i zasoby.
30) **Zapisy** – wszelkie udokumentowane informacje przechowywane zarówno w formie papierowej, jak i elektronicznej.
31) **Zdarzenie związane z bezpieczeństwem informacji** – wystąpienie stanu systemu, usługi, sieci, który wskazuje na możliwe naruszenie bezpieczeństwa informacji, brak kontroli lub brak odpowiednich procedur.

32) **Zasób informacyjny** – zob. aktywa informacyjne.

IV. Kontekst organizacji

[Zrozumienie organizacji i jej kontekstu]

§ 5. 1 Celem działalności Urzędu jest obsługa i zapewnienie pomocy organom Gminy, w realizacji ich zadań własnych, zleconych, wykonywanych na podstawie porozumień z organami administracji rządowej, powierzonych w drodze porozumień międzygminnych lub z powiatem, które nie zostały powierzone gminnym jednostkom organizacyjnym, związkom komunalnym lub przekazane innym podmiotom na podstawie umów.

2. Działalność Urzędu musi być realizowana zgodnie z aktami wewnętrznymi, w sposób sprawny, niezakłócony i terminowy.

[Zrozumienie potrzeb i oczekiwań stron zainteresowanych]

§ 6. 1. Burmistrz, na dzień przyjęcia niniejszego dokumentu, określił kontekst zewnętrzny i wewnętrzny działalności Urzędu, który wpływa na zdolność do osiągnięcia zamierzonych celów. Określając kontekst zewnętrzny i wewnętrzy Burmistrz wziął pod uwagę następujące elementy takie jak:

1) w zakresie kontekstu zewnętrznego: środowisko społeczne, kulturowe, polityczne, prawne, regulacyjne, finansowe, technologiczne, ekonomiczne, naturalne, konkurencyjne, czynniki mające wpływ na cele działalności Urzędu, relacje z zewnętrznymi interesariuszami i ich postrzeganie w zakresie pracy Urzędu oraz wartości,
2) w zakresie kontekstu wewnętrznego: zarządzanie, strukturę, podział ról, polityki, cele, strategie, posiadane zasoby (potencjał) relacje w wewnętrznymi interesariuszami, kulturę organizacyjną, system informacyjny i procesy, standardy, wytyczne i modele stosowane w Urzędzie, formy i zakres relacji umownych.

2. Zewnętrzny kontekst działalności Urzędu wyznaczają cele i oczekiwania następujących stron:

1) mieszkańcy - oczekiwanie realizacji zadań publicznych Burmistrza, Rady, komisji oraz innych organów funkcjonujących w strukturze Urzędu lub Gminy zgodnie z prawem, w sposób sprawny, niezakłócony i w wyznaczonym terminie.

2) starostwo powiatowe, województwo, organy administracji rządowej - oczekiwanie realizacji powierzonych zadań zgodnie z prawem, w sposób sprawny, niezakłócony i w wyznaczonym terminie.
3) miejskie jednostki organizacyjne – zapewnienie wsparcia merytorycznego, administracyjnego i ekonomicznego.
4) organizacje samorządowe i lokalne - zapewnienie wsparcia administracyjnego i ekonomicznego dla działalności organizacji.

2. Wewnętrzny kontekst działalności Urzędu wyznaczają cele i oczekiwania następujących stron:

1) Rada Miejska – realizacja zadań Urzędu wynikających ze statutu oraz uchwał rady, nadzorowanie pracy Burmistrza oraz podległych mu jednostek organizacyjnych.
2) Najwyższe kierownictwo – bezpieczeństwo zasobów informacyjnych, w tym unikanie i zapobieganie incydentom związanym z dostępem, modyfikacją, utratą bądź zniszczeniem informacji.
3) pracownicy – bezpieczeństwo i higiena pracy, dostępność i utrzymywanie sprawności środków wymiany informacji, uzyskiwanie informacji na poziomie umożliwiającym sprawne realizowanie powierzonych zadań.

3. Potrzeby i oczekiwania zainteresowanych stron będą brane pod uwagę w ramach ciągłego doskonalenia, a następnie przeglądane i aktualizowane w miarę upływu czasu.

[Określanie zakresu systemu zarządzania bezpieczeństwem informacji. Klasyfikacja zasobów informacyjnych]

§ 7. 1. Granice SZBI wyznaczają zewnętrzne i wewnętrzne czynniki kontekstu oraz oczekiwania zainteresowanych stron.

2. SZBI chroni wszelkie aktywa informacyjne poprzez zapewnienie ich poufności, dostępności, integralności, a także rozliczalności w ich zakresie i zgodności ich przetwarzania z prawem.

3. SZBI odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, przeglądania, utrzymywania i doskonalenia zarządzania bezpieczeństwem zasobów informacyjnych.

4. Zakres SZBI dotyczy obsługi mieszkańców, ludności i podmiotów gospodarczych oraz zarządzania przestrzenią Urzędu.

5. Zakres określony przez dokumenty SZBI ma zastosowanie do całego Urzędu i wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informacyjnych, w których przetwarzane są:

1) Informacje publiczne – informacje ogólnodostępne (dostępne publicznie).
2) Informacje ustawowo chronione – informacje, których ujawnienie może wiązać się z sankcjami karnymi, administracyjnymi lub odszkodowawczymi. Do informacji ustawowo chronionych należy zaliczyć dane osobowe, informacje niejawne, informacje objęte tajemnicą zawodową, skarbową, handlową, bankową, pracodawcy, przedsiębiorstwa, itp.
3) Informacje wewnętrzne:
   a) informacje wewnętrzne publiczne – informacje dostępne dla wszystkich pracowników bez względu na realizowane zadania,
   b) informacje wewnętrzne ograniczone - informacje dostępne dla części pracowników upoważnionych z uwagi na realizowane zadania,
   c) informacje wewnętrzne ustawowo chronione – informacje chronione przepisami prawa.

[System zarządzania bezpieczeństwem informacji]

§ 8. Urząd ustanawia, wdraża, utrzymuje i stale doskonali SZBI zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017-06.

V. Przywództwo

[Przywództwo i zaangażowanie]

§ 9. 1. Urząd zobowiązuje się do utrzymania wysokich standardów bezpieczeństwa informacji poprzez ciągłe doskonalenie procesów, zwiększanie świadomości pracowników oraz zapewnienie poufności, integralności i dostępności zasobów informacyjnych dla zainteresowanych stron.

2. Urząd będzie oceniać ryzyko dla bezpieczeństwa informacji na podstawie wartości aktywów, zagrożeń i słabych punktów. Jeśli wartość ryzyka jest bardzo wysoka, zostaną wdrożone odpowiednie zabezpieczenia.

§ 10. 1. Najwyższe kierownictwo musi wykazać się przywództwem i zaangażowaniem w odniesieniu do systemu zarządzania bezpieczeństwem informacji poprzez:

1) zapewnienie, że polityka bezpieczeństwa informacji i cele bezpieczeństwa informacji są ustanowione i są zgodne ze strategicznym kierunkiem Urzędu,
2) zapewnienie integracji wymagań SZBI z procesami Urzędu,
3) zapewnienie dostępności zasobów niezbędnych dla SZBI,
4) informowanie o znaczeniu skutecznego zarządzania bezpieczeństwem informacji oraz zgodności z wymaganiami SZBI,
5) zapewnienie, że SZBI osiąga zamierzone cele,
6) kierowanie i wspieranie osób przyczyniających się do zwiększenia skuteczności SZBI,
7) promowanie ciągłego doskonalenia oraz wspieranie innych właściwych ról kierowniczych w celu zademonstrowania ich wiodącej roli.

3. Ponadto, Urząd:

1) wdraża procedury mające na celu zachowanie poufności, integralności i dostępności wszystkich zasobów informacyjnych.
2) wychwytuje incydenty związane z bezpieczeństwem informacji, kontroluje działalność i efektywność SZBI oraz stara się ciągle go doskonalić.
3) zapobiega zdarzeniom związanym z bezpieczeństwem informacji oraz buduje i rozwija SZBI w celu zapewnienia poufności, integralności i dostępności informacji.
4) respektuje wartość informacji dotyczących swoich pracowników i zabezpiecza je.
5) zapewnia wszystkim pracownikom odpowiednie szkolenia w celu utrzymania i poprawy skuteczności SZBI.
6) ustanawia plan ciągłości działania w celu zabezpieczenia kontynuacji działalności, przy założeniu wystąpienia dysfunkcji systemów informatycznych, jak również klęski żywiołowej, aktów terroryzmu, rozprzestrzeniania się choroby zakaźnej na dużą skalę, itp.

[Polityka]

§ 11. 1. W trosce o bezpieczeństwo informacji, w tym danych podlegających ochronie zgodnie z właściwymi przepisami, mając świadomość ich znaczenia dla funkcjonowania Urzędu Burmistrz Gminy Żychlin ustanowił system zarządzania bezpieczeństwem informacji (SZBI) zgodny z normą PN-EN ISO/IEC 27001:2017-06, zobowiązał się do spełnienia

wymagań wskazanej normy i ciągłego doskonalenia SZBI oraz zadeklarował przeznaczenie zasobów i kompetencji niezbędnych dla jego prawidłowego funkcjonowania, jak również zobowiązał się udzielenia wsparcia do podejmowania wszelkich działań prowadzących do kompleksowego zabezpieczenia aktywów i zasobów informacyjnych objętych zakresem SZBI.

2. PBI ma służyć jako dokument referencyjny opisujący ramy bezpieczeństwa przyjęte przez Urząd.

3. Dokument ten jest dostępny dla wszystkich stron zainteresowanych.

4. Obowiązkiem Urzędu jest zatwierdzenie, opublikowanie i podanie do wiadomości niniejszego dokumentu wszystkim jej pracownikom i właściwym stronom zewnętrznym.

[Role, odpowiedzialność i uprawnienia]

§ 12. 1. Urząd jest zaangażowany w bezpieczeństwo informacji i ciągłe doskonalenie SZBI.

2. Najwyższe kierownictwo dostarcza dowodów swojego zaangażowania w ustanowienie, wdrożenie, funkcjonowanie, monitorowanie, przegląd, utrzymanie i doskonalenie SZBI poprzez:

1) ustanowienie PBI,
2) ustanowienie celów i pomiarów ich realizacji oraz planów w zakresie bezpieczeństwa informacji,
3) ustalenie ról i obowiązków w zakresie bezpieczeństwa informacji,
4) przekazanie pracownikom Urzędu informacji w zakresie spełniania celów bezpieczeństwa informacji i zgodności z PBI, poinformowanie o ich obowiązkach wynikających z przepisów prawa oraz o potrzebie ciągłego doskonalenia,
5) zapewnienie wystarczających zasobów do ustanowienia, wdrożenia, obsługi, monitorowania, przeglądu, utrzymania i doskonalenia SZBI,
6) podejmowanie decyzji w sprawie kryteriów akceptacji ryzyka i akceptowalnego poziomu ryzyka,
7) zapewnienie przeprowadzania wewnętrznych i zewnętrznych audytów SZBI,
8) przeprowadzanie przeglądów zarządzania SZBI.

VI. Planowanie

[Działania odnoszące się do ryzyk i szans]

[Postanowienia ogólne]

§ 13. 1. Podczas planowania SZBI Urząd uwzględnia swój kontekst oraz potrzeby i oczekiwania stron zainteresowanych, a także określa ryzyka i szanse, które należy uwzględnić:

1) zapewnienie poufności, integralności i dostępności informacji,
2) unikanie lub ograniczania niepożądanych skutków incydentów i zdarzeń związanych z bezpieczeństwem informacji,
3) ciągłe doskonalenie.

2. Urząd planuje działania mające na celu zaradzenie tym zagrożeniom i szansom oraz sposoby zintegrowania i wdrożenia działań w ramach procesów systemu zarządzania bezpieczeństwem informacji. Urząd przeprowadza ocenę skuteczności tych działań.

[Ocena ryzyka w bezpieczeństwie informacji]

§ 14. 1. Urząd określa i stosuje proces oceny ryzyka w zakresie bezpieczeństwa informacji, który:

1) ustanawia i utrzymuje kryteria ryzyka w zakresie bezpieczeństwa informacji, które obejmują:
   a) kryteria akceptacji ryzyka,
   b) kryteria przeprowadzania oceny ryzyka dla bezpieczeństwa informacji.
2) zapewnia, że powtarzane oceny ryzyka w zakresie bezpieczeństwa informacji dają spójne, ważne i porównywalne wyniki.
3) identyfikuje ryzyko związane z bezpieczeństwem informacji:
   a) proces oceny ryzyka związanego z bezpieczeństwem informacji w celu identyfikacji zagrożeń związanych z utratą poufności, integralności i dostępności informacji w ramach SZBI,
   b) zidentyfikowanie właścicieli ryzyka.
4) ocenia ryzyko związane z bezpieczeństwem informacji poprzez:
   a) ocenę potencjalnych konsekwencji, które wystąpiłyby w przypadku zmaterializowania się zidentyfikowanych ryzyk,
   b) ocenę realnego prawdopodobieństwa wystąpienia zidentyfikowanych ryzyk,
   c) określenie poziomu ryzyka.
5) ocenia ryzyko związane z bezpieczeństwem informacji poprzez:

a) porównywanie wyników oceny ryzyka z ustalonymi kryteriami ryzyka,

b) uszeregowanie zidentyfikowanych zagrożeń pod względem ważności w celu minimalizowania ryzyka.

2. Urząd dokumentuje informacje dotyczące procesu oceny ryzyka związanego z bezpieczeństwem informacji.

3. Proces oceny ryzyka został opisany w Polityce oceny i zarządzania ryzykiem.

[Postępowanie z ryzykiem w bezpieczeństwie informacji]

§ 15. 1. Urząd określa i stosuje proces zarządzania ryzykiem poprzez:

1) wybór odpowiednich opcji postępowania z ryzykiem związanym z bezpieczeństwem informacji, z uwzględnieniem wyników oceny ryzyka,
2) określenie wszystkich kontroli (mechanizmów kontrolnych), które są niezbędne do wdrożenia wybranej opcji postępowania z ryzykiem związanym z bezpieczeństwem informacji.

[Cele bezpieczeństwa informacji i planowanie ich osiągnięcia]

§ 16. 1. Urząd ustala cele w zakresie bezpieczeństwa informacji na odpowiednich funkcjach i poziomach. Cele w zakresie bezpieczeństwa informacji:

1) są zgodne z polityką bezpieczeństwa informacji,
2) są wymierne (jeżeli jest to wykonalne),
3) uwzględniają obowiązujące wymogi w zakresie bezpieczeństwa informacji oraz wynikają z oceny ryzyka,
4) są przekazywane,
5) w razie potrzeby podlegają aktualizacji.

2. Urząd przechowuje udokumentowane informacje dotyczące celów w zakresie bezpieczeństwa informacji. Poniżej przedstawiono główne cele SZBI ustanowione przez najwyższe kierownictwo:

1) zapewnienie ochrony informacji przed nieupoważnionym dostępem,
2) zapewnienie poufności, dostępności i integralności informacji zgodnie z wymaganiami prawnymi,
3) zapewnienie, że wszelkie naruszenia bezpieczeństwa informacji oraz jego słabe punkty są raportowane i badane,

4) zapewnienie, że zachowanie ciągłości realizacji zadań publicznych odbywa się w oparciu o udokumentowane plany, weryfikowane i testowane w stopniu umożliwiającym potwierdzenie ich przydatności,
5) zapewnienie wysokiej świadomości pracowników w zakresie bezpieczeństwa informacji.

VII. Wsparcie

[Zasoby]

§ 17. 1. Najwyższe kierownictwo zapewnia środki na wdrożenie, utrzymanie i przegląd SZBI. Zasoby te obejmują fundusze, narzędzia, zasoby ludzkie i wszelkie inne zasoby, które mogą być niezbędne do skutecznego funkcjonowania SZBI.

2. Urząd okresowo ocenia zapotrzebowanie na zasoby w celu poprawy infrastruktury bezpieczeństwa w oparciu o ocenę ryzyka oraz audyty bezpieczeństwa informacji. W oparciu o zapotrzebowanie na zasoby najwyższe kierownictwo zatwierdza lub/i przydziela wymagane zasoby.

[Kompetencje]

§ 18. 1. Do zarządzania SZBI przydzielane są osoby, które mają doświadczenie, umiejętności i wiedzę w dziedzinie bezpieczeństwa informacji.

2. Gdy wymagane poziomy doświadczenia, umiejętności i wiedzy w zakresie bezpieczeństwa informacji nie są dostępne, Urząd realizuje działania podnoszące świadomość w zakresie bezpieczeństwa informacji, które zapewniają doskonalenie umiejętności i rozwijanie wiedzy dotyczącej tej dziedziny.

3. Urząd zapewnia odpowiednie kompetencje w dziedzinie bezpieczeństwa informacji poprzez:

1) określenie, jakie działania podnoszące świadomość są potrzebne i z jaką częstotliwością należy je realizować,
2) identyfikowanie wykwalifikowanych osób lub dostawców do realizowania działań podnoszących świadomość,
3) organizowanie programu działań podnoszących świadomość,
4) zbieranie informacji zwrotnych dotyczących działań podnoszących świadomość.

4. Urząd dokumentuje działania podnoszące świadomość w zakresie bezpieczeństwa informacji.

[Uświadamianie]

§ 19. 1. Pracownicy Urzędu muszą być zapoznani z treścią PBI oraz na bieżąco informowani o wszystkich aktualizacjach dotyczących PBI i procedur Urzędu, które są dla nich istotne.

2. Pracownicy muszą być świadomi ich wkładu w skuteczność SZBI, w tym korzyści płynących z poprawy wyników w zakresie bezpieczeństwa informacji.

3. Pracownicy muszą mieć świadomość konsekwencji w przypadku wystąpienia braku zgodności z wymogami SZBI.

[Komunikacja]

§ 20. Pracownicy są informowani o ryzyku związanym z bezpieczeństwem informacji za pośrednictwem wszelkich kanałów komunikacji dostępnych w Urzędzie. Przy wyborze kanału komunikacji należy każdorazowo kierować się adekwatnością, dostępnością i szybkością obiegu informacji.

[Udokumentowane informacje]

[Postanowienia ogólne]

§ 21. SZBI obejmuje:

1) udokumentowane informacje wymagane przez normę PN-EN ISO/IEC 27001:2017-06,
2) udokumentowane informacje określone przez Urząd jako niezbędne dla skuteczności SZBI.

[Opracowywanie i aktualizowanie]

§ 22. Podczas tworzenia i aktualizowania udokumentowanych informacji pracownicy muszą uwzględnić poniższe właściwości:

1) identyfikacja i opis (np. tytuł, datę, autora lub numer referencyjny),
2) format (np. język, wersja oprogramowania, grafika),
3) nośnik (np. papierowy, elektroniczny),
4) dostępność,
5) przydatność,
6) adekwatność.

[Nadzór nad udokumentowanymi informacjami]

§ 23. 1. Udokumentowane informacje wymagane przez SZBI oraz przez normę PN-EN ISO/IEC 27001:2017-06 są kontrolowane w celu zapewnienia:

1) dostępności i odpowiedniego wykorzystania, tam gdzie i kiedy są potrzebne,
2) że SZBI jest odpowiednio chroniony (np. przed utratą poufności, niewłaściwym wykorzystaniem lub utratą integralności).

2. W celu kontroli udokumentowanych informacji podejmuje się następujące działania, stosownie do przypadku:

1) dystrybucję, dostęp, wyszukiwanie i wykorzystanie informacji,
2) przechowywanie, w tym zachowanie czytelności informacji,
3) kontrolę zmian (np. kontrolę wersji),
4) zatrzymanie i rozdysponowanie informacji.

3. Udokumentowane informacje pochodzenia zewnętrznego, określone przez Urząd jako niezbędne do planowania i działania SZBI, są odpowiednio identyfikowane i kontrolowane. Dostęp oznacza decyzję dotyczącą zezwolenia na przeglądanie jedynie udokumentowanych informacji lub zezwolenia i upoważnienia do przeglądania i zmiany udokumentowanych informacji itp.

§ 24. 1. Wszystkie dokumenty związane z wymaganiami SZBI są kontrolowane poprzez:

1) przegląd i zatwierdzanie dokumentów pod kątem adekwatności przed ich wydaniem lub wykorzystaniem,
2) aktualizację, przegląd i zatwierdzanie niezbędnych zmian w kontrolowanych dokumentach,
3) dostępność aktualnych przeglądów niezbędnych dokumentów,
4) wycofanie nieaktualnych dokumentów w celu zapewnienia ochrony przed niezamierzonym użyciem,
5) wszystkie dokumenty zabezpieczające powinny być dostępne do wglądu i wykorzystania w oparciu o wymogi niezbędnej wiedzy.

2. W ramach każdej procedury w SZBI identyfikuje się zapisy w celu dostarczenia dowodów na zgodność z wymogami i skuteczne funkcjonowanie SZBI.

VIII. Działania operacyjne

[Planowanie i nadzór nad działaniami operacyjnymi]

§ 25. 1. Wybrane cele kontroli oraz kontrole (zabezpieczenia) stanowiące część planu postępowania z ryzykiem są skutecznie wdrażane w Urzędzie, a także umożliwiają szybkie wykrywanie i reagowanie na zdarzenia naruszające bezpieczeństwo informacji.

2. Urząd zapewnia prowadzenie odpowiednich szkoleń i podnoszenie świadomości w zakresie SZBI oraz przydzielanie odpowiednich zasobów do zarządzania SZBI.

3. Urząd utrzymuje odpowiednią matrycę ograniczania ryzyka / incydentów, identyfikowaną do celów monitorowania, aby zapewnić skuteczność podejmowanych działań. Prowadzone są rejestry minimalizacji ryzyka lub/i incydentów w celu porównania wyników i ich odtworzenia.

§ 26. 1. Urząd zapewnia, że SZBI jest odpowiednio monitorowany i okresowo poddawany przeglądowi.

2. W zakresie monitorowania incydentów Urząd posiada zdefiniowaną procedurę zarządzania incydentami, która zapewnia, że wszystkie problemy, błędy zidentyfikowane podczas przetwarzania jakichkolwiek informacji są obsługiwane szybko i skutecznie, a naruszenie bezpieczeństwa jest odpowiednio rozwiązywane.

3. Urząd przeprowadza przeglądy SZBI i zapewnia audyty. Celem przeglądów i audytów jest zapewnienie, że SZBI jest skuteczny, a wszystkie polityki, kontrole i cele bezpieczeństwa są zgodne z założeniami. Audyt SZBI koncentruje się na zgodności z praktykami Urzędu określonymi w SZBI i jest wykonywany przez niezależnych audytorów.

4. Należy dokonywać przeglądu poziomu dopuszczalnego i pozostałego ryzyka w odniesieniu do zmian we wdrożonej technologii, nowych zagrożeń i słabych punktów oraz celów związanych z działalnością Urzędu.

5. Wyniki okresowych ocen ryzyka powinny być ze sobą zestawiane i porównywane w celu weryfikacji skuteczności kontroli.

§ 27. 1. Zabezpieczenia systemów informacyjnych są wdrażane i włączane do SZBI w oparciu o:

1) sprawozdania z przeglądów SZBI,
2) ustalenia z audytów bezpieczeństwa informacji.

2. Odpowiednie działania naprawcze i zapobiegawcze podejmowane są na podstawie:

1) sprawozdania z przeglądów SZBI,
2) ustalenia z audytów bezpieczeństwa informacji,

3) raportów o incydentach,
4) zmian środowiskowych (nowych zagrożeń, słabych punktów, zmian technologicznych, itp.).

[Szacowanie ryzyka w bezpieczeństwie informacji]

§ 28. Urząd dokonuje oceny ryzyka w zakresie bezpieczeństwa informacji zgodnie z przyjętą Polityką oceny i zarządzania ryzykiem w planowanych odstępach czasu lub w przypadku zaproponowania lub wystąpienia istotnych zmian, biorąc pod uwagę ustalone kryteria. Urząd dokumentuje informacje o wynikach ocen ryzyka w zakresie bezpieczeństwa informacji.

[Postępowanie z ryzykiem w bezpieczeństwie informacji]

§ 29. Urząd wdraża plan postępowania z ryzykiem w zakresie bezpieczeństwa informacji. Urząd dokumentuje informacje o wynikach przetwarzania ryzyka związanego z bezpieczeństwem informacji.

IX. Ocena wyników

[Monitorowanie, pomiary, analiza i ocena]

§ 30. 1. Pełnomocnik ds. SZBI ocenia wydajność bezpieczeństwa informacji i skuteczność SZBI. Pełnomocnik ds. SZBI dokonuje ustaleń:

1) co należy monitorować i mierzyć, w tym ocenia procesy i kontrole (zabezpieczenia) w zakresie bezpieczeństwa informacji,
2) metod monitorowania, pomiaru, analizy i oceny, w stosownych przypadkach, w celu zapewnienia prawidłowych wyników z uwzględnieniem poniższych postanowień.

2. Wyniki monitorowania i pomiarów są analizowane i oceniane co najmniej raz w roku. Analiza ta może być jednak przeprowadzona częściej, w zależności od potrzeb.

3. Urząd przechowuje odpowiednie udokumentowane informacje stanowiące dowód monitorowania i przeprowadzania pomiarów.

4. **W celu zapewnienia ochrony informacji przed nieuprawnionym dostępem** przyjmuje się za wskaźnik pomiaru wydajności i skuteczności SZBI ilość incydentów powiązanych z umożliwieniem dostępu osób nieuprawnionych do informacji (np. pozostawienie dokumentacji chronionej bez dozoru, pozostawienie osób nieuprawnionych bez dozoru, pozostawienie sprzętu bez dozoru, próby włamania do systemów informacyjnych, itp.)

w danym roku. Dąży się do ilości incydentów równej zeru w ciągu każdego roku kalendarzowego.

5. **W celu zapewnienia poufności, dostępności i integralności informacji zgodnie z wymaganiami prawnymi** przyjmuje się za wskaźnik pomiaru wydajności i skuteczności SZBI ilość ryzyk nieakceptowalnych przez najwyższe kierownictwo wykazanych podczas procesu oceny ryzyka (analizy ryzyka) dla grup informacji, których wagę (poufność, dostępność lub integralność) oszacowano na poziomie 3. Dąży się do wyeliminowania ryzyk nieakceptowalnych do końca pierwszej połowy danego roku.

6. **W celu zapewnienia, że wszelkie naruszenia bezpieczeństwa informacji oraz jego słabe punkty są raportowane i oceniane** przyjmuje się za wskaźnik pomiaru ilość działań naprawczych zakończonych pomyślnie (działania naprawcze po wystąpieniu naruszenia, które przyniosły zamierzone skutki), podjętych po zgłoszeniu naruszenia wobec ogólnej liczby naruszeń wykrytych w danym roku. Dąży się do 80% skuteczności podjętych działań naprawczych do końca pierwszej połowy każdego roku.

7. **W celu zapewnienia, że zachowanie ciągłości realizacji zadań publicznych odbywa się w oparciu o udokumentowane plany, weryfikowane i testowane w stopniu umożliwiającym potwierdzenie ich przydatności** przyjmuje się za wskaźnik pomiaru pozytywne wyniki z przeprowadzonych testów ciągłości działania. Dąży się do podtrzymania najważniejszych systemów informacyjnych przez co najmniej 15 min działania w razie braku dostaw prądu a ich odtworzenie może zająć nie więcej niż 12 godzin roboczych.

8. **W celu zapewnienia wysokiej świadomości pracowników** przyjmuje się za wskaźnik pomiaru ilość pozytywnie przeprowadzonych testów świadomości pracowników (testy wiedzy). Za pozytywny wynik testu uznaje się odpowiednią reakcję pracownika na przeprowadzony scenariusz lub udzielenie prawidłowej odpowiedzi. **Dąży się do** 60% pozytywnie zaliczonych testów wiedzy w obszarze bezpieczeństwa informacji dla danego pracownika.

4. **[Audyt wewnętrzny]**

§ 31. 1. Urząd przeprowadza raz w roku audyty SZBI. Audyty te są przeprowadzane w celu zapewnienia, że SZBI jest:

1) zgodny z wymaganiami normy PN-EN ISO/IEC 27001:2017-06 lub/i powiązanymi,
2) zgodny z odpowiednimi wymogami prawnymi, ustawowymi i umownymi,

3) zgodny z określonymi wymogami bezpieczeństwa informacji,
4) skutecznie wdrażany, utrzymywany i nadzorowany aby wprowadzać działania mające na celu jego doskonalenie i eliminowanie nieprawidłowości,
5) funkcjonuje zgodnie z oczekiwaniami.

2. Audyt SZBI jest przeprowadzony przez niezależnych audytorów, którzy nie ponoszą bezpośredniej odpowiedzialności za działania będące przedmiotem audytu.

3. Sekretarz lub osoba upoważniona przez najwyższe kierownictwo sporządza zakres audytu na dany rok przed końcem roku poprzedniego i niezwłocznie udostępnia informację kierownikom komórek organizacyjnych objętych audytem. Zakres audytu ustala się w taki sposób, aby uwzględnić w nim:

1) wagę poszczególnych elementów SZBI dla celów Urzędu,
2) problemy występujące w praktyce działania Urzędu w obszarze poszczególnych elementów SZBI lub danej komórki organizacyjnej Urzędu,
3) komórki organizacyjne Urzędu objęte audytem, jeżeli audyt nie dotyczy całego Urzędu.

5. Audyt dokumentuje się na karcie audytu, która powinna zawierać informacje dotyczące audytowanej komórki organizacyjnej Urzędu, termin audytu, osobę audytora, odnotowane spostrzeżenia lub niezgodności. Audytor sporządza listę pytań kontrolnych obejmującą zakres audytu. Audytor wpisuje na kartę audytu spostrzeżenia oraz stwierdzone niezgodności, które omawia z przedstawicielem audytowanej komórki organizacyjnej Urzędu i uzyskuje od niego pisemne potwierdzenie na karcie audytu. Stwierdzone niezgodności mogą być usunięte w trakcie audytu, o ile są naprawialne a fakt ten wpisuje się do karty audytu jako spostrzeżenie.

7. Audytor przeprowadza audyt zbierając obiektywne dowody.

8. Niezwłocznie po zakończeniu audytu, audytor przekazuje Pełnomocnikowi ds. SZBI kartę audytu wraz z listą pytań kontrolnych i ewentualnymi notatkami oraz omawia z nim wyniki audytu. Pełnomocnik ds. SZBI dokonuje przeglądu zapisów na karcie audytu i związanej z audytem dokumentacji a następnie podejmuje decyzję w sprawie podjęcia działań korygujących.

Pełnomocnik ds. SZBI przechowuje wszystkie zapisy dotyczące audytu oraz działań korygujących przez okres zgodny z instrukcją kancelaryjną.

[Przegląd zarządzania]

§ 32. 1. Najwyższe kierownictwo dokonuje raz w roku przeglądu zarządzania lub na podstawie incydentów lub zdarzeń związanych z bezpieczeństwem informacji, aby zapewnić jego stałą przydatność, adekwatność i skuteczność. Przegląd zarządzania obejmuje analizę:

1) statusu działań z poprzednich przeglądów SZBI,
2) zmian w kwestiach zewnętrznych i wewnętrznych, które są istotne dla SZBI,

2. Przegląd zarządzania musi dostarczać informacji zwrotnych oraz kierunków w zakresie:

1) niezgodności i działań naprawczych,
2) wyników monitorowania i pomiarów,
3) wyników audytów,
4) realizacji celów w zakresie bezpieczeństwa informacji,
5) informacji zwrotnych od zainteresowanych stron,
6) wyników oceny ryzyka i planu postępowania z ryzykiem,
7) szans na ciągłe doskonalenie.

3. Wyniki przeglądu zarządzania obejmują decyzje związane z możliwościami ciągłego doskonalenia oraz wszelkie potrzeby w zakresie zmian w SZBI.

4. Urząd przechowuje udokumentowane wyniki jako dowody przeprowadzania przeglądów zarządzania.

X. Doskonalenie

[Niezgodność i działania korygujące]

§ 33. 1. W przypadku wystąpienia niezgodności należy:

1) podjąć reakcję i w stosownych przypadkach:
   a) podjąć działania mające na celu jej kontrolę i usunięcie,
   b) zminimalizować lub zneutralizować jej skutki,
2) ocenić potrzebę podjęcia działań w celu wyeliminowania przyczyn niezgodności, tak aby nie powtórzyły się one lub nie wystąpiły gdzie indziej, poprzez:
   a) dokonanie przeglądu niezgodności,
   b) określenie przyczyn niezgodności,
   c) określenie, czy podobne niezgodności istnieją lub mogą potencjalnie wystąpić,
3) wdrożyć wszelkie niezbędne działania naprawcze,

4) dokonać przeglądu skuteczności wszelkich podjętych działań naprawczych,

5) w razie potrzeby dokonać zmian w SZBI.

2. Działania naprawcze muszą być odpowiednie do skutków napotkanych niezgodności. Organizacja przechowuje udokumentowane informacje jako dowody:

1) charakter niezgodności i wszelkich późniejszych podjętych działań naprawczych,

2) wyniki wszelkich działań naprawczych.

[Ciągłe doskonalenie]

§ 34. Urząd jest odpowiedzialny za ciągłe doskonalenie SZBI pod kątem jego przydatności i skuteczności. Wkładem do ciągłego doskonalenia mogą być:

1) zmiany w PBI i celach bezpieczeństwa,

2) wyniki audytu wewnętrznego SZBI i sprawozdania z przeglądu zarządzania,

3) raporty o incydentach,

4) analiza monitorowanych zdarzeń,

5) działania naprawcze i zapobiegawcze,

6) zmiany środowiskowe (nowe zagrożenia i podatności).

Załącznik nr 1. Deklaracja Stosowania (DS)

A.5 Polityki bezpieczeństwa informacji		
A.5.1 Kierunki bezpieczeństwa informacji określane przez kierownictwo		
Cel: Zapewnienie przez kierownictwo wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji, zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami.		
A.5.1.1	Polityki bezpieczeństwa informacji	Zabezpieczenie **jest** stosowane.
A.5.1.2	Przegląd polityk bezpieczeństwa informacji	Zabezpieczenie **jest** stosowane.
A.6 Organizacja bezpieczeństwa informacji		
A.6.1 Organizacja wewnętrzna		
Cel: Ustanowić strukturę zarządzania w celu zainicjowania oraz nadzorowania, wdrażania i eksploatacji bezpieczeństwa informacji w organizacji.		
A.6.1.1	Role i odpowiedzialność za bezpieczeństwo informacji	Zabezpieczenie **jest** stosowane.
A.6.1.2	Rozdzielanie obowiązków	Zabezpieczenie **jest** stosowane.
A.6.1.3	Kontakty z organami władzy	Zabezpieczenie **jest** stosowane.
A.6.1.4	Kontakty z grupami zainteresowanych specjalistów	Zabezpieczenie **jest** stosowane.
A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	Zabezpieczenie **jest** stosowane.

A.6.2 Urządzenia mobilne i telepraca		
Cel: Zapewnić bezpieczeństwo telepracy i stosowania urządzeń mobilnych.		
A.6.2.1	Polityka stosowania urządzeń mobilnych	Zabezpieczenie **jest** stosowane.
A.6.2.2	Telepraca	Zabezpieczenie **jest** stosowane.
A.7 Bezpieczeństwo zasobów ludzkich		
A.7.1 Przed zatrudnieniem		
Cel: Zapewnić, żeby pracodawcy i kontrahenci rozumieli swoją odpowiedzialność i byli odpowiednimi kandydatami do wypełnienia ról do których są przewidziani.		
A.7.1.1	Postępowanie sprawdzające	Zabezpieczenie **jest** stosowane.
A.7.1.2	Warunki zatrudnienia	Zabezpieczenie **jest** stosowane.
A.7.2 Podczas zatrudnienia		
Cel: Zapewnić, żeby pracownicy i kontrahenci byli świadomi swoich obowiązków dotyczących bezpieczeństwa informacji i wypełniali je.		
A.7.2.1	Odpowiedzialność kierownictwa	Zabezpieczenie **jest** stosowane.
A.7.2.2	Uświadomienie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Zabezpieczenie **jest** stosowane.
A.7.2.3	Postępowanie dyscyplinarne	Zabezpieczenie **jest** stosowane.
A.7.3 Zakończenie i zmiana zatrudnienia		
Cel: Zabezpieczyć interesy organizacji w trakcie procesu zmiany lub zakończenia zatrudnienia.		
A.7.3.1	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	Zabezpieczenie **jest** stosowane.
A.8 Zarządzanie aktywami		
A.8.1 Odpowiedzialność za aktywa		
Cel: Zidentyfikować aktywa organizacji i zdefiniować właściwą odpowiedzialność w dziedzinie ich ochrony.		
A.8.1.1	Inwentaryzacja zasobów	Zabezpieczenie **jest** stosowane.
A.8.1.2	Własność aktywów	Zabezpieczenie **jest** stosowane.
A.8.1.3	Akceptowalne użycie aktywów	Zabezpieczenie **jest** stosowane.
A.8.1.4	Zwrot aktywów	Zabezpieczenie **jest** stosowane.
A.8.2 Klasyfikacja informacji		
Cel: Zapewnić przypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla organizacji.		
A.8.2.1	Klasyfikowanie informacji	Zabezpieczenie **jest** stosowane.
A.8.2.2	Oznaczanie informacji	Zabezpieczenie **jest** stosowane.
A.8.2.3	Postępowanie z aktywami	Zabezpieczenie **jest** stosowane.
A.8.3 Postępowanie z nośnikami		
Cel: Zapobiec nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji zapisanych na nośnikach.		
A.8.3.1	Zarządzanie nośnikami wymiennymi	Zabezpieczenie **jest** stosowane.
A.8.3.2	Wycofywanie nośników	Zabezpieczenie **jest** stosowane.
A.8.3.3	Przekazywanie nośników	Zabezpieczenie **jest** stosowane.
A.9 Kontrola dostępu		
A.9.1 Wymagania biznesowe wobec kontroli dostępu		
Cel: Ograniczyć dostęp do informacji i środków przetwarzania informacji.		

A.9.1.1	Polityka kontroli dostępu	Zabezpieczenie **jest** stosowane.
A.9.1.2	Dostęp do sieci i usług sieciowych	Zabezpieczenie **jest** stosowane.
A.9.2 Zarządzenie dostępem użytkowników		
Cel: Zapewnić dostęp uprawnionym użytkownikom i zapobiec nieuprawnionemu dostępowi do systemu i usług.		
A.9.2.1	Rejestrowanie i wyrejestrowywanie użytkowników	Zabezpieczenie **jest** stosowane.
A.9.2.2	Przydzielanie dostępu użytkownikom	Zabezpieczenie **jest** stosowane.
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu	Zabezpieczenie **jest** stosowane.
A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	Zabezpieczenie **jest** stosowane.
A.9.2.5	Przegląd praw dostępu użytkowników	Zabezpieczenie **jest** stosowane.
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu	Zabezpieczenie **jest** stosowane.
A.9.3 Odpowiedzialność użytkowników		
Cel: Zapewnić rozliczalność użytkowników przez ochronę ich informacji uwierzytelniających.		
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających	Zabezpieczenie **jest** stosowane.
A.9.4 Kontrola dostępu do systemów i aplikacji		
Cel: Zapobiec nieuprawnionemu dostępowi do systemów i aplikacji.		
A.9.4.1	Ograniczanie dostępu do informacji	Zabezpieczenie **jest** stosowane.
A.9.4.2	Procedury bezpiecznego logowania	Zabezpieczenie **jest** stosowane.
A.9.4.3	System zarządzania hasłami	Zabezpieczenie **jest** stosowane.
A.9.4.4	Użycie uprzywilejowanych programów narzędziowych	Zabezpieczenie **jest** stosowane.
A.9.4.5	Kontrola dostępu do kodów źródłowych programów	Zabezpieczenie **jest** stosowane.
A.10 Kryptografia		
A.10.1 Zabezpieczenia kryptograficzne		
Cel: Zapewnić właściwe i skuteczne wykorzystanie kryptografii do ochrony poufności, autentyczności i/lub integralności informacji.		
A.10.1.1	Polityka stosowania zabezpieczeń kryptograficznych	Zabezpieczenie **jest** stosowane.
A.10.1.2	Zarządzanie kluczami	Zabezpieczenie **jest** stosowane.
A.11 Bezpieczeństwo fizyczne i środowiskowe		
A.11.1 Obszary bezpieczne		
Cel: Zapobiec nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach i środkach przetwarzania informacji należących do organizacji.		
A.11.1.1	Fizyczna granica obszaru bezpiecznego	Zabezpieczenie **jest** stosowane.
A.11.1.2	Fizyczne zabezpieczenie wejść	Zabezpieczenie **jest** stosowane.
A.11.1.3	Zabezpieczenie biur, pomieszczeń i obiektów	Zabezpieczenie **jest** stosowane.

A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Zabezpieczenie **jest** stosowane.
A.11.1.5	Praca w obszarach bezpiecznych	Zabezpieczenie **jest** stosowane.
A.11.1.6	Obszary dostaw i załadunku	Zabezpieczenie **jest** stosowane.
A.11.2 Sprzęt		
Cel: Zapobiec utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.		
A.11.2.1	Lokalizacja i ochrona sprzętu	Zabezpieczenie **jest** stosowane.
A.11.2.2	Systemy wspomagające	Zabezpieczenie **jest** stosowane.
A.11.2.3	Bezpieczeństwo okablowania	Zabezpieczenie **jest** stosowane.
A.11.2.4	Konserwacja sprzętu	Zabezpieczenie **jest** stosowane.
A.11.2.5	Wynoszenie aktywów	Zabezpieczenie **jest** stosowane.
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą	Zabezpieczenie **jest** stosowane.
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	Zabezpieczenie **jest** stosowane.
A.11.2.8	Pozostawianie sprzętu użytkownika bez opieki	Zabezpieczenie **jest** stosowane.
A.11.2.9	Polityka czystego biurka i czystego ekranu	Zabezpieczenie **jest** stosowane.
A.12. Bezpieczna eksploatacja		
A.12.1 Procedury eksploatacyjne i odpowiedzialność		
Cel: Zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji.		
A.12.1.1	Dokumentowanie procedur eksploatacyjnych	Zabezpieczenie **jest** stosowane.
A.12.1.2	Zarządzanie zmianami	Zabezpieczenie **jest** stosowane.
A.12.1.3	Zarządzanie pojemnością	Zabezpieczenie **jest** stosowane.
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Zabezpieczenie **jest** stosowane.
A.12.2 Ochrona przed szkodliwym oprogramowaniem		
Cel: Zapewnić informacjom i środkom przetwarzania informacji ochronę przed szkodliwym oprogramowaniem.		
A.12.2.1	Zabezpieczenia przed szkodliwym oprogramowaniem	Zabezpieczenie **jest** stosowane.
A.12.3 Kopie zapasowe		
Cel: Chronić przed utratą danych.		
A.12.3.1	Zapasowe kopie informacji	Zabezpieczenie **jest** stosowane.
A.12.4 Rejestrowanie zdarzeń i monitorowanie		
Cel: Rejestrować zdarzenia i zbierać materiał dowodowy.		
A.12.4.1	Rejestrowanie zdarzeń	Zabezpieczenie **jest** stosowane.
A.12.4.2	Ochrona informacji w dziennikach zdarzeń	Zabezpieczenie **jest** stosowane.
A.12.4.3	Rejestrowanie działań administratorów i operatorów	Zabezpieczenie **jest** stosowane.
A.12.4.4	Synchronizacja zegarów	Zabezpieczenie **jest** stosowane.
A.12.5 Nadzór nad oprogramowaniem produkcyjnym		
Cel: Zapewnić integralność systemów produkcyjnych.		

A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych	Zabezpieczenie **jest** stosowane.
A.12.6 Zarządzanie podatnościami technicznymi		
Cel: Zapobiec wykorzystaniu podatności technicznych.		
A.12.6.1	Zarządzanie podatnościami technicznymi	Zabezpieczenie **jest** stosowane.
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	Zabezpieczenie **jest** stosowane.
A.12.7 Rozważania dotyczące audytu systemów informacyjnych		
Cel: Zminimalizować wpływ działań audytu na systemy produkcyjne.		
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych	Zabezpieczenie **jest** stosowane.
A.13 Bezpieczeństwo komunikacji		
A.13.1 Zarządzanie bezpieczeństwem sieci		
Cel: Zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania informacji.		
A.13.1.1	Zabezpieczenia sieci	Zabezpieczenie **jest** stosowane.
A.13.1.2	Bezpieczeństwo usług sieciowych	Zabezpieczenie **jest** stosowane.
A.13.1.3	Rozdzielanie sieci	Zabezpieczenie **jest** stosowane.
A.13.2 Przesyłanie informacji		
Cel: Utrzymać bezpieczeństwo informacji przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi.		
A.13.2.1	Polityki i procedury przesyłania informacji	Zabezpieczenie **jest** stosowane.
A.13.2.2	Porozumienia dotyczące przesyłania informacji	Zabezpieczenie **jest** stosowane.
A.13.2.3	Wiadomości elektroniczne	Zabezpieczenie **jest** stosowane.
A.13.2.4	Umowy o zachowaniu poufności	Zabezpieczenie **jest** stosowane.
A.14 Pozyskiwanie, rozwój i utrzymanie systemów		
A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych		
Cel: Zapewnić, żeby bezpieczeństwo informacji było nieodłączną częścią systemów informacyjnych w całym cyklu życia. Dotyczy to również wymagań wobec systemów informacyjnych dostarczających usług w sieciach publicznych.		
A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji	Zabezpieczenie **jest** stosowane.
A.14.1.2	Zabezpieczenie usług aplikacyjnych w sieciach publicznych	Zabezpieczenie **jest** stosowane.
A.14.1.3	Ochrona transakcji usług aplikacyjnych	Zabezpieczenie **jest** stosowane.
A.14.2 Bezpieczeństwo w procesach rozwoju i wsparcia		
Cel: Zapewnić projektowanie i wdrożenie bezpieczeństwa informacji w ramach cyklu życia systemów informacyjnych.		
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych	Zabezpieczenie **jest** stosowane.
A.14.2.2	Procedury kontroli zmian w systemach	Zabezpieczenie **jest** stosowane.

A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	Zabezpieczenie **jest** stosowane.
A.14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania	Zabezpieczenie **jest** stosowane.
A.14.2.5	Zasady projektowania bezpiecznych systemów	Zabezpieczenie **jest** stosowane.
A.14.2.6	Bezpieczne środowisko rozwojowe	Zabezpieczenie **jest** stosowane.
A.14.2.7	Prace rozwojowe zlecane podmiotom zewnętrznym	Zabezpieczenie **jest** stosowane.
A.14.2.8	Testowanie bezpieczeństwa systemów	Zabezpieczenie **jest** stosowane.
A.14.2.9	Testy akceptacyjne systemów	Zabezpieczenie **jest** stosowane.
A.14.3. Dane testowe		
Cel: Zapewnić ochronę danych stosowanych do testów.		
A.14.3.1	Ochrona danych testowych	Zabezpieczenie **jest** stosowane.
A.15 Relacje z dostawcami		
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami		
Cel: Zapewnić ochronę aktywów organizacji udostępnianych dostawcom.		
A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z dostawcami	Zabezpieczenie **jest** stosowane.
A.15.1.2	Uwzględnienie bezpieczeństwa w porozumieniach z dostawcami	Zabezpieczenie **jest** stosowane.
A.15.1.3	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	Zabezpieczenie **jest** stosowane.
A.15.2 Zarządzanie usługami dostarczanymi przez dostawców		
Cel: Utrzymać uzgodniony poziom bezpieczeństwa informacji i świadczonych usług zgodnie z umowami z dostawcami.		
A.15.2.1	Monitorowanie i przegląd usług świadczonych przez dostawców	Zabezpieczenie **jest** stosowane.
A.15.2.2	Zarządzanie zmianami w usługach świadczonych przez dostawców.	Zabezpieczenie **jest** stosowane.
A.16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji		
A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami		
Cel: Zapewnić, spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji, z uwzględnieniem informowania o zdarzeniach i słabościach.		
A.16.1.1	Odpowiedzialność i procedury	Zabezpieczenie **jest** stosowane.
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Zabezpieczenie **jest** stosowane.
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji	Zabezpieczenie **jest** stosowane.
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	Zabezpieczenie **jest** stosowane.

A.16.1.5	Reagowanie na incydenty związane z bezpieczeństwem informacji	Zabezpieczenie **jest** stosowane.
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	Zabezpieczenie **jest** stosowane.
A.16.1.7	Gromadzenie materiału dowodowego	Zabezpieczenie **jest** stosowane.
A.17 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania		
A.17.1 Ciągłość bezpieczeństwa informacji		
Cel: Zaleca się uwzględnienie ciągłości bezpieczeństwa informacji w systemach zarządzania ciągłością działania organizacji.		
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji	Zabezpieczenie **jest** stosowane.
A.17.1.2	Wdrożenie ciągłości bezpieczeństwa informacji	Zabezpieczenie **jest** stosowane.
A.17.1.3	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	Zabezpieczenie **jest** stosowane.
A.17.2 Nadmiarowość		
Cel: Zapewnić dostępność środków przetwarzania informacji.		
A.17.2.1	Dostępność środków przetwarzania informacji	Zabezpieczenie **jest** stosowane.
A.18 Zgodność		
A.18.1 Zgodność z przepisami prawnymi i umownymi		
Cel: Unikać naruszania zobowiązań prawnych, regulacyjnych lub umownych związanych z bezpieczeństwem informacji oraz innych wymagań dotyczących bezpieczeństwa.		
A.18.1.1	Określenie stosownych wymagań prawnych i umownych	Zabezpieczenie **jest** stosowane.
A.18.1.2	Prawa własności intelektualnej	Zabezpieczenie **jest** stosowane.
A.18.1.3	Ochrona zapisów	Zabezpieczenie **jest** stosowane.
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę	Zabezpieczenie **jest** stosowane.
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	Zabezpieczenie **jest** stosowane.
A.18.2 Przeglądy bezpieczeństwa informacji		
Cel: Zapewnić zgodnie z politykami organizacji i procedurami wdrożenie i stosowanie zasad bezpieczeństwa informacji.		
A.18.2.1	Niezależny przegląd bezpieczeństwa informacji	Zabezpieczenie **jest** stosowane.
A.18.2.2	Zgodność z politykami bezpieczeństwa i normami	Zabezpieczenie **jest** stosowane.
A.18.2.3	Sprawdzanie zgodności technicznej	Zabezpieczenie **jest** stosowane.

BURMISTRZ
Grzegorz Ambroziak