Regionalna Zintegrowana Infrastruktura Informacji Przestrzennej
Aglomeracji Kalisko-Ostrowskiej

Polityka Bezpieczeństwa Systemu Regionalna Zintegrowana Infrastruktura Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej.

Zatwierdzam.....

PREZYDENT
MIASTA KALISZA
Krystian Kinastowski

REJESTR ZMIAN DOKUMENTU

WERSJA	DATA	MODYFIKACJA
1.0	2021-03-01	WERSJA PIERWOTNA

I. Ogólna Polityka Bezpieczeństwa dla użytkowników Systemu Regionalna Zintegrowana Infrastruktura Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej.

§ 1 – Postanowienia ogólne.

1. Niniejszy dokument składa się z trzech części wraz z załącznikami:
   1) Ogólna Polityka Bezpieczeństwa dla użytkowników Systemu Regionalna Zintegrowana Infrastruktura Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej – dla wszystkich użytkowników oraz administratorów.
   2) Instrukcja zarządzania Systemem Regionalna Zintegrowana Infrastruktura Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej – dla Głównych ASI oraz Lokalnych ASI.
   3) Instrukcja administrowania Systemem Regionalna Zintegrowana Infrastruktura Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej – dla administratorów głównych Systemu.
2. Kierownicy JST AKO obejmują Regionalną Zintegrowaną Infrastrukturę Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej obowiązującym w ich jednostkach systemem zarządzania bezpieczeństwem informacji zapewniającym poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność, o którym mowa w § 20 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.
3. Za bezpieczeństwo informacji przetwarzanych w Systemie Regionalnej Zintegrowanej Infrastruktury Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej, zwanym dalej „Systemem RZIIP AKO" odpowiedzialny jest każdy uzyskujący do niej dostęp poprzez stosowanie przepisów niniejszej „Polityki Bezpieczeństwa Regionalnej Zintegrowanej Infrastruktury Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej", zwanej dalej „Polityką Bezpieczeństwa", przepisów dotyczących ochrony danych osobowych oraz obowiązujących użytkowników RZIIP AKO dokumentów wewnętrznych dotyczących bezpieczeństwa informacji i ochrony danych osobowych. Przez przepisy dotyczące ochrony danych osobowych należy rozumieć w szczególności przepisy rozporządzenia Parlamentu

Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych) (Dz. Urz. UE L 119/1 z 4.5.2016), zwanego dalej „RODO", przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000) wraz z przepisami wykonawczymi oraz przepisy odrębnych ustaw, które odnoszą się do przetwarzanych w systemie RZIIP AKO danych osobowych.

4. Niniejsza Polityka Bezpieczeństwa, składa się na dokumentację opisującą środki techniczne i organizacyjne ustanowione żeby przetwarzanie danych osobowych odbywało się zgodnie z RODO. Środki te będą poddawane przeglądom i uaktualniane.
5. Niniejsza Polityka Bbezpieczeństwa normuje zagadnienia związane z bezpieczeństwem informacji gromadzonych, przetwarzanych, transmitowanych lub przechowywanych w systemie teleinformatycznym RZIIP AKO, z którego korzystają JST AKO.
6. W szczególności Polityka Bezpieczeństwa określa sposób korzystania z Systemu RZIIP AKO oraz jego zabezpieczenia przed dostępem do nich osób nieupoważnionych.
7. Opisane i zastosowane zabezpieczenia mają zapewnić w szczególności:
   1) poufność informacji – rozumianą jako właściwość zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym;
   2) integralność informacji – rozumianą jako właściwość zapewniającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
   3) dostępność informacji – rozumianą jako właściwość zapewniającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym.
8. W zakresie nieuregulowanym w niniejszej Polityce Bezpieczeństwa zastosowanie mają obowiązujące użytkowników Systemu RZIIP AKO przepisy wewnętrzne danej jednostki dotyczące bezpieczeństwa informacji i ochrony danych osobowych.
9. Wszyscy Użytkownicy Systemu RZIIP AKO zobowiązani są do zapoznania się z Polityką Bezpieczeństwa.

§ 2 – Pojęcia.

1. Przez użyte w niniejszej Polityce Bezpieczeństwa pojęcia należy rozumieć:

1) JST AKO – jednostka samorządu terytorialnego Aglomeracji Kalisko-Ostrowskiej, korzystająca z Systemu RZIIP AKO;
2) kierownik JST AKO – Starosta, Prezydent Miasta, Burmistrz lub Wójt danej JST AKO;
3) kierownik komórki organizacyjnej – Naczelnik Wydziału, Dyrektor Wydziału, Kierownik Biura, samodzielne stanowisko pracy, kierownik wymienionej w Regulaminie Organizacyjnym danego Urzędu lub równorzędnej komórki organizacyjnej Urzędu o innej nazwie;
4) RZIIP AKO – Regionalna Zintegrowana Infrastruktura Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej;
5) System RZIIP AKO – Infrastruktura teleinformatyczna składająca się ze sprzętu i oprogramowania komputerowego, stanowiąca jednolite środowisko służące do gromadzenia, przetwarzania i udostępniania informacji przestrzennej wdrożonej w technologii GIS, dla potrzeb Regionalnej Zintegrowanej Infrastruktury Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej;
6) Główny ASI – Administrator główny systemu informatycznego „Regionalna Zintegrowana Infrastruktura Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej" odpowiedzialny za zapewnienie jego działania i zabezpieczenie tego systemu informatycznego, wyznaczony przez Prezydenta Miasta Kalisza;
7) Lokalny ASI – osoba wyznaczona przez kierownika JST AKO odpowiedzialna za zapewnienie działania i zabezpieczenie systemu RZIIP AKO w danej JST AKO;
8) dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
9) przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

10) podmiot zewnętrzny (podmiot przetwarzający) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który świadczy usługi na rzecz JST AKO (przetwarza dane osobowe w imieniu JST AKO);
11) użytkownik – pracownik posiadający uprawnienia do pracy w Systemie RZIIP AKO zgodnie z zakresem obowiązków służbowych, użytkownik z uprawnieniami na poziomie administratora staje się administratorem systemu;
12) współpracownik – inna niż pracownik JST AKO osoba mająca dostęp do Systemu RZIIP AKO np. stażysta, praktykant, podmiot zewnętrzny (podmiot przetwarzający);
13) zabezpieczenie systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem, ujawnieniem lub pozyskaniem danych, a także ich utratą;
14) incydent bezpieczeństwa informacji – pojedyncze zdarzenie lub seria zdarzeń związanych z bezpieczeństwem informacji, które zagrażają ich integralności, dostępności i poufności;
15) hasło – słowo złożone z liter, cyfr lub innych znaków, które musi podać użytkownik aby mógł korzystać z dostępu do zastrzeżonych zasobów np. sieci komputerowej, bazy danych, komputera. Hasło jest jednym ze sposobów ochrony danych przed osobami nieupoważnionymi;
16) naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
17) postępowanie z ryzykiem – wdrażanie środków i działań mających na celu minimalizację wystąpienia ryzyka;

§ 3 – Kierownictwo.

1. Prezydent Miasta Kalisza zapewnia warunki umożliwiające właściwe funkcjonowanie Systemu RZIIP AKO.
2. Kierownik JST AKO zapewnia warunki umożliwiające właściwe funkcjonowanie Systemu RZIIP AKO w zakresie swojej jednostki.

3. Kierownik JST AKO, jako właściciel danych przetwarzanych w podległej jemu jednostce pełni funkcję ich administratora i jest odpowiedzialny za ich bezpieczeństwo oraz przetwarzanie zgodnie z obowiązującymi przepisami.
4. Kierownik JST AKO, jest Administratorem danych Systemu RZIIP AKO właściwych jednostce i odpowiada za ich rzetelność i aktualność.
5. Do obowiązków Kierownika JST AKO w zakresie bezpieczeństwa informacji Systemu RZIIP AKO należy w szczególności:
   1) wnioskowanie o nadanie uprawnień dla podległych pracowników do Systemu RZIIP AKO i określenie zakresu tych uprawnień;
   2) akceptacja wniosków kierowników komórek organizacyjnych danego Urzędu, o nadanie uprawnień dla podległych pracowników do Systemu RZIIP AKO, w których przetwarzane są dane, których jest właścicielem lub gdy nie jest właścicielem a przetwarza dane te na podstawie porozumień, umów lub ustawowych udostępnień;
   3) aktywny udział w procesie reagowania na incydenty bezpieczeństwa informacji (w tym naruszenia ochrony danych osobowych) i podejmowanie działań związanych z odpowiedzialnością pracowniczą wobec podległych pracowników odpowiedzialnych za incydenty (naruszenia);
   4) zapoznanie użytkowników Systemu RZIIP AKO „Polityki Bezpieczeństwa Regionalnej Zintegrowanej Infrastruktury Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej".
   5) zapewnienie przestrzegania niniejszej Polityki Bezpieczeństwa oraz przepisów dotyczących ochrony danych osobowych przez podległych pracowników.

§ 4 – Pracownicy uzyskujący dostęp do Systemu RZIIP AKO.

1. Do obowiązków pracowników uzyskujący dostęp do informacji przetwarzanych w Systemie RZIIP AKO w zakresie bezpieczeństwa informacji i ochrony danych osobowych należy w szczególności:
   1) przestrzeganie zasad bezpieczeństwa informacji określonych w Polityce Bezpieczeństwa;
   2) przetwarzanie danych osobowych zgodnie z przepisami dotyczącymi ochrony danych osobowych;
   3) niezwłoczne informowanie o incydentach bezpieczeństwa informacji.

§ 5 – Inne osoby uzyskujące dostęp do Systemu RZIIP AKO.

1. Dostęp do informacji przetwarzanych w RZIIP AKO obok pracowników JST RZIIP AKO mogą mieć również inne osoby, zwane dalej „współpracownikami". Przepisy § 13 stosuje się odpowiednio do współpracowników z zastrzeżeniem § 4.

§ 6 – Zwalnianie i zmiana stanowiska pracy, zmiana zakresu dostępu.

1. Rozwiązanie stosunku pracy lub zmiana stanowiska pracy powiązana ze zmianą zakresu dostępu do danych, wymaga wycofania uprawnień do Systemu RZIIP AKO zgodnie z procedurą cofnięcia uprawnień użytkownika do Systemu RZIIP AKO – załącznik nr 5, oraz wypełnieniem wniosku modyfikacji użytkownika – załącznik nr 6.
2. Dla zmiany zakresu dostępu do danych Systemu RZIIP AKO przetwarzanych przez pracownika JST AKO, należy stosować procedurę modyfikacji uprawnień do Systemu RZIIP AKO – załącznik nr 4, oraz wypełnieniem wniosku modyfikacji użytkownika – załącznik nr 6.

§ 8 – Podmioty zewnętrzne uzyskujące dostęp do Systemu RZIIP AKO.

1. W przypadku podjęcia przez JST AKO współpracy z podmiotem zewnętrznym, która wiąże się z nadaniem jego pracownikom uprawnień do Systemu RZIIP AKO współpraca ta jest nawiązywana w oparciu o zawartą na piśmie umowę określającą m. in. zasady bezpieczeństwa. Za zawarcie umowy odpowiada kierownik JST AKO.
2. Jeżeli współpraca o której mowa w ust. 1 związana jest z powierzeniem podmiotowi zewnętrznemu danych osobowych umowa powinna spełniać wymagania określone w art. 28 RODO. Podmiot taki powinien zapewnić wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO. Oceny należy dokonać przed podjęciem decyzji o skorzystaniu z usług tego podmiotu.
3. Informacja o zawarciu umowy, o której mowa w ust. 1 musi być przekazana do Głównego ASI.
4. Kwestie związane z wykorzystywaniem Systemu RZIIP AKO do przekazywania danych do podmiotów zewnętrznych podlegają szczegółowym uregulowaniom w zawieranych obustronnie umowach, których procedury i klauzule dotyczące bezpieczeństwa systemów

informatycznych, winny być zgodne z uregulowaniami niniejszej Polityki oraz uzyskać akceptację Głównego ASI.

§ 9 – Znajomość zasad bezpieczeństwa informacji i świadomość.

1. Każdy użytkownik Systemu RZIIP AKO zobowiązany jest zapoznać się z Polityką Bezpieczeństwa. Wzór Oświadczenia o zapoznaniu się z „Polityką Bezpieczeństwa Regionalnej Zintegrowanej Infrastruktury Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej" stanowi załącznik nr 1 do Polityki Bezpieczeństwa.

§ 10 – Poufność.

1. Każdy uzyskujący dostęp do informacji przetwarzanych w Systemie RZIIP AKO (użytkownik) zobowiązany jest do zachowania w tajemnicy wszystkich danych do których ma dostęp (o ile nie są to dane jawne) oraz sposobów ich zabezpieczenia, zarówno w trakcie zatrudnienia jak i po jego ustaniu. Obowiązek zachowania tajemnicy obowiązuje również po ustaniu okoliczności uzasadniających nadanie uprawnień.
2. W przypadku umowy z podmiotem zewnętrznym, który otrzyma dostęp do Systemu RZIIP AKO zobowiązanie do zachowania w tajemnicy udostępnianych danych (o ile nie są to dane jawne), stanowi element tej umowy.

§ 11 – Odpowiedzialność.

1. Nie przestrzeganie przepisów Polityki Bezpieczeństwa stanowi naruszenie obowiązków pracowniczych i skutkuje odpowiedzialnością przewidzianą w obowiązującym w JST AKO Regulaminie Pracy (Kodeksie Pracy). Nie przestrzeganie przepisów dotyczących ochrony danych osobowych może dodatkowo skutkować odpowiedzialnością przewidzianą w przepisach ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

§ 12 – Dostęp do Systemu RZIIP AKO.

1. Dostęp do Systemu RZIIP AKO możliwy jest na podstawie nadanych uprawnień, po pomyślnym uwierzytelnieniu użytkownika. Metodą uwierzytelnienia jest podanie identyfikatora użytkownika i hasła.
2. Informacje w Systemie RZIIP AKO, o ile nie dotyczy to danych dostępnych publicznie, mogą przetwarzać tylko osoby upoważnione, którym nadano odpowiednie uprawnienia.
3. Procedura nadawania uprawnień do Systemu RZIIP AKO stanowi załącznik nr 3 Polityki Bezpieczeństwa.
4. Nadanie uprawnień do Systemu RZIIP AKO musi być uzasadnione zakresem przyznanych pracownikowi na piśmie zadań.
5. Uprawnienia do Systemu RZIIP AKO nadaje Główny ASI lub Lokalny ASI danej JST AKO na podstawie wypełnionego wniosku – załącznik nr 6.
6. Właściciel konta odpowiedzialny jest za wszelkie działania wykonane z użyciem jego identyfikatora.
7. Główny ASI prowadzi wykaz, zgodny z załącznikiem nr 2, zawierający zestawienie uprawnień oraz grup uprawnień.
8. Zabrania się:
   1) łamanie haseł,
   2) dokonywanie włamań na konta innych Użytkowników Systemu RZIIP AKO,
   3) nieprawne uzyskiwanie dostępu do kont administracyjnych,
   4) zakłócanie działania usług,
   5) omijanie i badania zabezpieczeń (za wyjątkiem działań związanych z audytem lub testowaniem systemu),
   6) praca na koncie innego użytkownika Systemu RZIIP AKO,
   7) podejmowanie innych działań mogących być zagrożeniem dla Systemu RZIIP AKO.

§ 13 – Polityka haseł.

1. Hasło musi mieć długość co najmniej 8 znaków oraz zawierać kombinację co najmniej trzech spośród następujących rodzajów znaków:
   1) małe litery;
   2) wielkie litery;

3) cyfry;
4) znaki specjalne np. !@#).

2. Ze względów technicznych w haśle użytkownika nie mogą być używane spacje i polskie znaki diakrytyczne (ł, ą, ć, ź, ó, itp.).
3. Użytkownik jest zobowiązany do zmiany hasła do Systemu RZIIP AKO nie rzadziej niż co 30 dni.
4. Kolejne hasła muszą być różne.
5. W przypadku zagubienia hasła, jego zapomnienia bądź ujawnienia osobie trzeciej, użytkownik zobowiązany jest do jego natychmiastowej zmiany. W przypadku braku możliwości samodzielnej zmiany hasła użytkownik zwraca się osobiście do Głównego ASI lub Lokalnego ASI danej JST AKO z wnioskiem o jego zmianę. Pracownik ten ma prawo do sprawdzenia tożsamości osób występujących o zmianę hasła.
6. W trakcie logowania do systemu hasło należy wprowadzać w sposób uniemożliwiający zapoznanie się z nim przez inne osoby.
7. Hasła należy przechowywać w sposób gwarantujący ich poufność.
8. Zabrania się:
   1) przekazywania haseł użytkowników innym osobom, w tym współpracownikom;
   2) zapisywania haseł w formie jawnej na kartce i pozostawienie zapisanych na kartce haseł w dostępnym dla innych osób miejscu;
   3) wykorzystywania haseł użytkowników, które nie spełniają minimalnych norm określonych w powyższym dokumencie.
9. Należy unikać wykorzystywania jako haseł:
   1) imion, nazwisk rodziny, dzieci, znajomych, współpracowników, zwierząt domowych;
   2) znanych postaci literackich, filmowych;
   3) popularnych nazw komputerowych;
   4) marek i numerów rejestracyjnych samochodu;
   5) dat urodzenia, dat historycznych;
   6) nazw użytkowników komputerów w żadnej postaci;
   7) nazw ulic, miast;
   8) wyrazów złożonych z sekwencji odczytywanej z klawiatury (np. qwerty, 12qwaszx);
   9) cech i numerów osobistych (np. dat urodzenia, imion itp.);
   10) identyfikatora użytkownika;
   11) popularnych wyrażeń językowych.
10. Hasła zachowują swoją poufność również po ustaniu ich czasu trwania.

§ 14 – Praca w Systemie RZIIP AKO.

1. Użytkownik rozpoczynając pracę w Systemie RZIIP AKO powinien zalogować się do systemu podając przyznany jemu identyfikator i hasło dostępu. Zabronione jest korzystanie z identyfikatora innego użytkownika.
2. Zawieszając pracę lub oddalając się od swojego stanowiska pracy użytkownik ma obowiązek wylogować się z Systemu RZIIP AKO lub uruchomić wygaszacz ekranu zabezpieczony hasłem uniemożliwiając osobom nieuprawnionym dostęp do danych (m. in. jednoczesne naciśnięcie klawiszy CTRL, ALT, DELETE i wybranie opcji zablokuj komputer).
3. Kończąc pracę w Systemie RZIIP AKO użytkownik powinien wylogować się.

§ 15 – Udostępnianie danych.

1. Informacje przetwarzane w Systemie RZIIP AKO udostępnia się na zasadach określonych w obowiązujących przepisach prawnych oraz wewnętrznych procedurach urzędu JST AKO.

§ 16 – Incydenty bezpieczeństwa informacji.

1. W przypadku wystąpienia incydentu bezpieczeństwa informacji związanego z funkcjonowaniem Systemie RZIIP AKO należy niezwłocznie o tym fakcie powiadomić Głównego ASI lub Lokalnego ASI. W przypadku poinformowania Lokalnego ASI powinien on niezwłocznie poinformować o tym fakcie Głównego ASI.
2. Główny ASI ustala czy incydent stanowi naruszenie ochrony danych osobowych oraz prowadzi postępowanie wyjaśniające w toku, którego ustala:
   1) czas wystąpienia incydentu;
   2) przyczyny wystąpienia incydentu;
   3) zakres incydentu (w przypadku naruszenia ochrony danych osobowych w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie);

4) skutki oraz wielkość szkód;
5) możliwe konsekwencje naruszenia ochrony danych osobowych;
6) środki jakie należy zastosować w celu zaradzenia naruszeniu ochrony danych osobowych lub w celu zminimalizowania jego ewentualnych negatywnych skutków.
7) dowody;
8) osoby odpowiedzialne za incydent.

3. Z przeprowadzonego postępowania wyjaśniającego Główny ASI sporządza Raport z naruszenia bezpieczeństwa i niezwłocznie przekazuje jego kopie właściwemu kierownikowi JST AKO.
4. W przypadku wystąpienia incydentu bezpieczeństwa informacji o którym mowa w ust. 1 stanowiącym naruszenie ochrony danych osobowych Główny ASI informuje o tym właściwego Inspektora ochrony danych. W takim przypadku zastosowanie mają przepisy dotyczące ochrony danych osobowych, wewnętrzne procedury obowiązujące w JST AKO, których bezpieczeństwo danych zostało naruszone oraz odpowiednie zapisy umowy powierzenia przetwarzania danych zawartych przez JST AKO z Miastem Kalisz.

§ 17 – Postanowienia końcowe i procedury.

1. Zobowiązuje się wszystkich Użytkowników Systemu RZIIP AKO do bezwzględnego przestrzegania ustaleń niniejszej polityki bezpieczeństwa.
2. Wszystkie procedury oraz wzory dokumentów, związane z Niniejszym dokumentem stanowią załączniki Polityki Bezpieczeństwa i muszą być użyte zgodnie z przeznaczeniem.

II. Instrukcja zarządzania Systemem Regionalna Zintegrowana Infrastruktura Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej. (dla Administratorów Systemu RZIIP AKO)

§ 1 – Administrator Systemu Informatycznego RZIIP AKO.

1. Głównym Administratorem Systemu Informatycznego RZIIP AKO, zwanym dalej Głównym ASI są wyznaczeni przez Prezydenta Miasta Kalisza pracownicy Urzędu Miasta Kalisza.
2. Lokalnym Administratorem Systemu Informatycznego RZIIP AKO, zwanym dalej Lokalnym ASI dla danej jednostki AKO jest wyznaczony przez kierownika JST AKO pracownik tej jednostki.
3. Główny ASI przydziela uprawnienia poszczególnym administratorom na piśmie, zgodnie z załącznikiem nr 7 oraz procedurą zgodną z załącznikiem nr 3.
4. Główny ASI modyfikuje, usuwa uprawnienia poszczególnym administratorom na piśmie, zgodnie z załącznikiem nr 7 oraz procedurą zgodną z załącznikiem nr 4 lub nr 5.
5. Główny ASI prowadzi wykaz wyznaczonych Lokalnych ASI, zgodny z załącznikiem nr 8.

§ 2 – Odpowiedzialność.

1. Główny ASI wraz z Lokalnymi ASI zabezpieczają sprawne działanie RZIIP AKO oraz sprawują nadzór nad wykonaniem umów związanych z funkcjonowaniem RZIIP AKO.
2. Główny ASI wraz Lokalnym ASI uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdraża odpowiednie środki techniczne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
3. Główny ASI wraz z Lokalnym ASI zapewnia przestrzeganie przepisów ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz wydanych na jej podstawie przepisów wykonawczych a w szczególności 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 (Dz. U. z 2017 r. poz. 2247).

4. Do podstawowych obowiązków Głównego ASI należy:
   1) zapewnienie ciągłości pracy Systemu RZIIP AKO;
   2) zarządzanie pracą Systemu RZIIP AKO, jego zasobami i użytkownikami;
   3) czuwanie nad bezpieczeństwem zasobów Systemu RZIIP AKO;
   4) zapewnienie kopii bezpieczeństwa i kopii archiwizacyjnych Systemu RZIIP AKO;
   5) współpraca z Lokalnymi ASI w celu właściwego zabezpieczenia działania i zabezpieczenia danych przetwarzanych w Systemie RZIIP AKO;
   6) konsultacje i zgłaszanie uwag o zauważonych anomaliach do odpowiedniej komórki informatycznej.
5. Do podstawowych obowiązków Lokalnego ASI należy:
   1) zapewnienie ciągłości działania lokalnych elementów Systemu RZIIP AKO, które zostały mu powierzone do administrowania;
   2) zarządzanie pracą lokalnych elementów Systemu RZIIP AKO, jego zasobami i użytkownikami;
   3) współpraca z Głównym ASI w celu właściwego zabezpieczenia działania i zabezpieczenia danych przetwarzanych w Systemie RZIIP AKO;
   4) konsultacje i zgłaszanie uwag o zauważonych anomaliach do Głównego ASI.

§ 3 – Konfiguracja sprzętu komputerowego.

1. Każdy komputer z którego uzyskiwany jest dostęp do Systemu RZIIP AKO jest wyposażony co najmniej w następujące oprogramowanie:
   1) aplikacje umożliwiającą dostęp do Systemu RZIIP AKO;
   2) system antywirusowy.

§ 4 – Zabezpieczenia sieci i urządzeń sieciowych

1. Urządzenia sieciowe zasila się z wydzielonej sieci elektrycznej odpowiednio zabezpieczonej urządzeniami UPS i systemami przeciwprzepięciowymi.

2. Stosuje się zasadę separacji sieci Systemu RZIIP AKO od sieci Internet za pomocą sprzętowej zapory wysokiej klasy, posiadającej funkcje blokowania portów, wykrywania wirusów, filtrowania treści oraz mechanizm wykrywania i zapobiegania włamaniom.
3. Zalecane jest zastosowanie zapory ogniowej (rozwiązanie sprzętowe lub programowe) oraz wdrożenie regulacji zapewniających jej bieżącą aktualizację.
4. Zaleca się zastosowanie 2 zapór ogniowych – sprzętowej na styku z siecią publiczną Internet oraz programowej na stacji roboczej, oraz wdrożenie regulacji zapewniających ich bieżącą aktualizację.
5. Dostęp do Systemu RZIIP AKO odbywa się za pośrednictwem szyfrowanego kanału VPN. Metoda ta stosowana jest do podłączenia JST AKO, firm świadczących usługi serwisowe i asystę techniczną oprogramowania oraz innych upoważnionych osób lub instytucji.
6. Zdalny dostęp do portów konfiguracyjnych i diagnostycznych jest możliwy tylko z lokalnej podsieci administracyjnej lub z dedykowanego tunelu VPN.
7. Przed nieautoryzowanym dostępem do środowiska sieciowego chronią:
   1) stosowanie Polityki haseł;
   2) ograniczenie dostępu z sieci Internet do niezbędnych zasobów, tylko w zakresie wybranych adresów, portów i protokołów; w tym celu stosuje się firewall, translację NAT, listy dostępowe skonfigurowane na zaporze;
   3) stosowanie tunelowania VPN do administrowania siecią i pracy zdalnej; połączenia VPN są skonfigurowane w sposób uniemożliwiający poszczególnym użytkownikom dostęp do innych zasobów (podsieci) niż niezbędne do wykonania wyznaczonych zadań;
   4) stosowanie filtrowania adresów IP na każdym etapie komunikacji pomiędzy podsieciami, a także – gdy jest to uzasadnione i możliwe – przy dostępie z zewnątrz;
   5) używanie oprogramowania zabezpieczającego przed typowymi atakami (np. przekierowaniem portów).
8. Sieć Systemu RZIIP AKO przed złośliwym oprogramowaniem chroni stosowanie na serwerach oraz innych komponentach sieci oprogramowania antywirusowego i jego regularna aktualizacja.
9. Wszystkie komputery z których umożliwiony jest dostęp do Systemu RZIIP AKO powinny być wyposażone w system antywirusowy posiadający funkcje automatycznej aktualizacji bazy wirusów, bieżącego skanowania każdego uruchomionego programu i otwieranego pliku. System antywirusowy posiada centralne zarządzanie i monitorowanie zdarzeń.

10. Urządzenia sieciowe pozwalające na dostęp do sieci Systemu RZIIP AKO powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich.
11. Administracja zdalna powinna być odpowiednio zabezpieczona przed nieuprawnionym dostępem za pomocą mechanizmów uwierzytelnienia routera (np. login i hasło o odpowiedniej złożoności).
12. Administracja zdalna powinna być uruchomiona wyłącznie na jednym porcie wewnętrznym, do którego ma dostęp wyłącznie Główny lub Lokalny ASI.
13. Zaleca się wdrożenie reglamentacji dostępu do sieci np. na podstawie adresów MAC.
14. Połączenie pomiędzy JST AKO z Systemem RZIIP AKO musi odbywać się za pomocą połączeń VPN.
15. Zdalny dostęp do serwerów w celach administracyjnych może być realizowany wyłącznie z użyciem narzędzi zapewniających bezpieczną komunikację – szyfrowania danych, tunelowania VPN z użyciem kluczy szyfrujących lub użycia certyfikatów.
16. Za techniczne umożliwienie Użytkownikom korzystania z zasobów Systemu RZIIP AKO oraz nadzorowanie i dbanie o bezpieczeństwo tego ruchu sieciowego, odpowiedzialny jest Główny ASI wraz Lokalnymi ASI.
17. Elementy Systemu RZIIP AKO służące do zautomatyzowanego przesłania danych pomiędzy JST AKO przy użyciu teletransmisji danych powinny być zabezpieczone mechanizmami szyfrującymi transmisję danych oraz powinny posiadać aktywne mechanizmy kontroli dostępu.
18. Zalecane jest włączenie automatycznych aktualizacji systemu oraz oprogramowania, zgodnie z zaleceniami producentów, a w przypadku braku dostępu do repozytorium poprawek online wdrożenie procedury aktualizacji systemu oraz oprogramowania na bieżąco.
19. Należy obowiązkowo stosować oprogramowanie antywirusowe oraz stosować ustawienia zapewniające aktualizację sygnatur antywirusowych na bieżąco lub w przypadku braku dostępu do sygnatur antywirusowych na bieżąco, wdrożyć procedury zapewniające aktualizację sygnatur antywirusowych nie rzadziej niż raz w tygodniu.
20. Klucze prywatne do certyfikatów VPN zainstalowanych w urządzeniu musza być zabezpieczone w sposób uniemożliwiający dostęp do nich oraz ich wykorzystanie przez osoby nieuprawnione
21. Do połączenia z sieciami Wi-Fi należy używać co najmniej standardu WPA.

§ 5 – Wymagania dotyczące sprzętu.

1. Stacje robocze przetwarzające dane w Systemie RZIIP AKO powinny być ustawiona w sposób uniemożliwiający do nich dostęp osobom nieupoważnionym.
2. Wymagane jest takie ustawienie monitora aby nie było możliwości podejrzenia danych przetwarzanych na ekranie przez osoby nieupoważnione.
3. Wymagane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków z Systemu RZIIP AKO przez osoby nieupoważnione.
4. Na stacjach roboczych przetwarzających dane w Systemie RZIIP AKO:
   1) powinno być zainstalowane oprogramowanie antywirusowe bieżąco aktualizowane, działające w czasie rzeczywistym;
   2) wymagane jest ustawienie czasu automatycznego uruchamiania wygaszacza użytkownika. Wznowienie pracy wymaga podania hasła, zalecane jest także blokowanie stacji przy każdorazowym opuszczeniu stanowiska;
   3) zalecane jest włączenie automatycznych aktualizacji systemu oraz oprogramowania zgodnie z zaleceniami producentów (opcja pobierz aktualizacje i zdecyduj kiedy/które zainstalować).

§ 6 – Zasady ochrony kryptograficznej.

1. W celu ochrony poufności przesyłanych oraz przechowywanych danych stosuje się zabezpieczenia kryptograficzne. Zabezpieczenia kryptograficzne występują w szczególności przy:
   1) wymianie danych z podmiotami zewnętrznymi;
   2) przesyłaniu informacji między lokalizacjami JST AKO.
2. Do szyfrowania połączeń stosuje się w szczególności:
   1) połączenia szyfrowane SSL/TLS;
   2) tunele VPN.
3. W systemach obsługujących transmisję ważnych danych należy używać kluczy kryptograficznych.
4. Za generowanie, przechowywanie i bezpieczną dystrybucję kluczy kryptograficznych odpowiada Główny ASI.

§ 7 – Zabezpieczenie Systemu RZIIP AKO przed zjawiskami fizycznymi.

1. Pomieszczenia, w których eksploatowane są urządzenia komputerowe, oraz pomieszczenia, w których przechowywane są dane, powinny być:
   1) wolne od zagrożeń związanych ze zjawiskami fizycznymi typu:
      a) wyładowania elektrostatyczne i atmosferyczne (np. elektryzujące się wykładziny, sąsiedztwo urządzeń odgromowych),
      b) silne działanie pól elektromagnetycznych (np. bliskie sąsiedztwo stacji transformatorowych i urządzeń rozdzielczych wysokiego napięcia, pól magnetycznych pochodzących od urządzeń z silnikami elektrycznymi wysokiej mocy lub od transformatorów zasilania budynków itp.),
   2) zabezpieczone systemem ochrony p.poż.,
   3) zabezpieczone przed zalaniem,
   4) zabezpieczone przed nieupoważnionym dostępem.
2. Pomieszczenia, w których zainstalowane są Serwery powinny mieć zapewnione stałe utrzymywanie temperatury, wilgotności i innych parametrów określonych przez producenta serwerów. Zabezpieczenie przed brakiem lub czasowym zanikiem prądu ma być zapewnione poprzez zastosowanie awaryjnych zasilaczy bezprzerwowych oraz źródła rezerwowego zasilania.
3. Miejsca, w których przechowywane są nośniki danych, powinny zapewniać ochronę przed czynnikami zewnętrznymi mogącymi doprowadzić do utraty danych.

§ 8 – Fizyczne zabezpieczenie Systemu RZIIP AKO przed dostępem osób nieupoważnionych.

1. Serwery, macierze dyskowe, urządzenia sieciowe i teletransmisyjne, szafy teletechniczne, wyłączniki zasilania elektrycznego, szafy z nośnikami magnetycznymi zawierające kopie danych powinny być usytuowane w pomieszczeniu uniemożliwiającym dostęp do nich osób nieupoważnionych, w szczególności:
   1) Dostęp do pomieszczeń, winien być ściśle kontrolowany poprzez zainstalowane systemy alarmowe (jeśli takowy jest zainstalowany) oraz kontrolę dostępu do pomieszczeń.

2) Serwery oraz komputery, w których zapisane są dane, w tym dane osobowe, winny być szczególnie zabezpieczone poprzez zastosowanie rozwiązań uniemożliwiających swobodne przemieszczanie oraz utrudniających ich ewentualny zabór.

2. Lokalizacja urządzeń komputerowych (komputerów typu PC i przenośnych) w pomieszczeniach użytkowanych przez Użytkowników Systemu RZIIP AKO powinna uniemożliwiać osobom postronnym dostęp do nich, a także wgląd do danych wyświetlanych na monitorach komputerowych.
3. Ograniczenie dostępu z ust. 2 nie dotyczy urządzeń przeznaczonych do samoobsługi osób nie będących użytkownikami Systemu RZIIP AKO, np. infokiosków, terminali informacyjnych.
4. Wszelkie prace konserwacyjne i naprawcze sprzętu RZIIP AKO oraz uaktualnienia lub naprawy Systemu RZIIP AKO, wykonywane przez firmę zewnętrzną, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy JST AKO, a tymże podmiotem, z uwzględnieniem klauzuli dotyczącej ochrony przez Zleceniobiorcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi.
5. W przypadku naprawy sprzętu komputerowego w serwisie zewnętrznym ważne dane należy zabezpieczyć (zarchiwizować) oraz o ile to możliwe usunąć z nośników informacji.

§ 9 – Zabezpieczenia sprzętu i oprogramowania.

1. Wszystkie urządzenia służące do przetwarzania informacji w Systemie RZIIP AKO tj. serwery, macierze dyskowe, urządzenia sieciowe i teletransmisyjne, urządzenia służące do konfiguracji sieci (routery, przełączniki), komputery, urządzenia peryferyjne (drukarki, skanery) umieszcza się w obszarze przetwarzania informacji w sposób uniemożliwiający dostęp do nich osób nieupoważnionych. Urządzenie peryferyjne należy rozmieszczać w taki sposób, aby nie dopuścić do sytuacji, w której osoby pracujące w pomieszczeniu, w których znajduje się urządzenie nie mają upoważnienia do przetwarzania informacji, która może być przetwarzana na tym urządzeniu przez innego użytkownika.
2. Ograniczenie dostępu z ust. 1 nie dotyczy urządzeń przeznaczonych do samoobsługi osób nie będących użytkownikami Systemu RZIIP AKO, np. infokiosków, terminali informacyjnych z ograniczonym dostępem osób trzecich.

3. Wszystkie serwery oraz urządzenia służące do konfiguracji sieci (routery, przełączniki) są zabezpieczonego urządzeniami UPS z mechanizmem automatycznego zamykania systemu w przypadku braku zasilania i systemami przeciwprzepięciowymi.
4. Pamięci masowe serwerów i macierze dyskowe są skonfigurowane w sposób zapobiegający utracie danych wskutek awarii dysków za pomocą kontrolerów RAID.
5. Serwery powinny znajdować się w zabezpieczonych systemem alarmowym klimatyzowanych pomieszczeniach. Dostęp do pomieszczeń mają tylko wybrane osoby.
6. Dostęp do systemów operacyjnych serwerów możliwy jest wyłącznie dla Głównego lub Lokalnego ASI po podaniu identyfikatora i hasła.
7. Dostęp do danych przetwarzanych w postaci elektronicznej możliwy jest po wielostopniowym uwierzytelnieniu użytkownika:
   1) dostęp do systemu operacyjnego wymaga pełnego uwierzytelnienia użytkownika (login i hasło);
   2) dostęp do Systemu RZIIP AKO wymaga pełnego uwierzytelnienia użytkownika (login i hasło).
8. Komputer powinien mieć uaktywnioną funkcją wygaszania ekranu po braku aktywności, z włączoną opcją wymuszania ponownego uwierzytelnienia użytkownika za pomocą hasła przy odblokowaniu.
9. System operacyjny każdego urządzenia musi być skonfigurowany w sposób wymuszający podanie hasła użytkownika w celu rozpoczęcia pracy w systemie.
10. Systemy operacyjne komputerów powinny być na bieżąco aktualizowane. Zmiany w systemach operacyjnych powinny być poprzedzone analizą wpływu tych zmian na krytyczne aplikacje. Analiza powinna być wykonana przy użyciu środowiska testowego.
11. W każdym systemie operacyjnym komputera musi być zainstalowane i aktywne oprogramowanie antywirusowe.
12. W administracji bazami danych nigdy nie są używane główne konta predefiniowane (root), z wyjątkiem pierwszej konfiguracji.
13. Wymagane jest takie ustawienie monitora, aby nie było możliwości podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione. Zalecane jest stosowanie filtrów prywatyzacyjnych zabezpieczających przed możliwością podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione.

14. Wymagane jest ustawienie czasu automatycznego uruchamiania wygaszacza, wznowienie pracy wymaga podania hasła, obowiązkowe jest blokowanie stacji przez Użytkownika przy każdorazowym opuszczeniu stanowiska.
15. Wymagane jest takie ustawienie drukarki, aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.
16. Stacja robocza powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieuprawnionym.

§ 10 – Tworzenie kont użytkowników i hasła.

1. Nazwa użytkownika musi spełniać wymagania odnośnie budowy wg wzorca: [dwuliterowy skrót nazwy JSTO AKO] _ [imię] . [nazwisko]
2. Każdemu użytkownikowi komputera ma być założone oddzielne konto, konta te nie powinny mieć przypisanych uprawnień administratora, o ile nie jest to wymagane do bieżącej pracy.
3. Każdy użytkownik Systemu RZIIP AKO musi posiadać unikalny adres email.
4. Każdy użytkownik Systemu RZIIP AKO posiada odrębny identyfikator nadany przez Głównego ASI lub Lokalnego ASI i hasło.
5. Identyfikator użytkownika pozostaje niezmieniony i nie może być przydzielony innej osobie.
6. Identyfikator wpisuje się do ewidencji osób którym nadano uprawnienia do Systemu RZIIP AKO prowadzonej przez Głównego ASI oraz rejestruje go w Systemie RZIIP AKO.
7. Właściwy do nadania uprawnień Główny ASI lub Lokalny ASI przekazuje identyfikator i wygenerowane hasło bezpośrednio użytkownikowi w formie ustnej lub pisemnej z pominięciem osób trzecich.
8. Użytkownik systemu, po otrzymaniu informacji o nadaniu uprawnień loguje się do Systemu RZIIP AKO w celu sprawdzenia poprawności konta i uprawnień. Długość nazwy użytkownika powinna wynosić nie mniej niż 3 znaki.
9. Hasło musi spełniać wymagania Polityki Haseł.
10. Główny ASI lub Lokalny ASI na wniosek użytkownika Systemu RZIIP AKO zmienia niezwłocznie jego hasło w przypadku stwierdzenia jego ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.
11. W przypadku prac serwisowych Główny ASI upoważniony jest do zresetowania hasła.

12. Kopia dokumentu potwierdzającego nadanie odpowiednich uprawnień do Systemu RZIIP AKO w JST AKO musi być przekazana do Głównego ASI.
13. Główny ASI prowadzi wykaz, zgodny z załącznikiem nr 9, zawierający zestawienie wydanych uprawnień.

§ 11 – Konta administracyjne.

1. Każdy administrator posługuje się własnym kontem administracyjnym i własnym hasłem w celu zapewnienia rozliczalności.
2. Wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora.
3. Hasło musi spełniać wymagania Polityki Haseł.
4. Hasła administracyjne są obowiązkowo zmieniane w każdym przypadku zmian kadrowych w gronie osób administrującym danym systemem.
5. Hasła służące do administrowania systemami i programami należy zmienić niezwłocznie, w przypadku stwierdzenia ich ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.
6. Hasła Użytkowników Systemu RZIIP AKO, należy zmienić niezwłocznie w przypadku stwierdzenia ich ujawnienia lub podejrzenia o ujawnienie osobie nieuprawnionej.
7. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła.

III. Instrukcja administrowania Systemem Regionalna Zintegrowana Infrastruktura Informacji Przestrzennej Aglomeracji Kalisko-Ostrowskiej. (dla Administratorów Głównych Systemu RZIIP AKO)

§ 1 – Umowy.

1. Umowy dotyczące świadczenia usług teleinformatycznych, zakupu lub modernizacji urządzeń komputerowych, systemów informatycznych i oprogramowania powinny zawierać niezbędne wymagania dotyczące bezpieczeństwa informacji lub odniesienia do odpowiednich dokumentów regulujących te kwestie w JST AKO oraz zakresy odpowiedzialności stron umowy w tym względzie.
2. W celu ograniczenia ryzyka niewydolności funkcjonalnej Systemu RZIIP AKO (pojemność Systemu RZIIP AKO) należy prognozować przyszłe wymagania dotyczące pojemności zasobów dyskowych, mocy obliczeniowej procesorów, przepustowości sieci itd. Wymagania te powinny być określone i udokumentowane przed zaakceptowaniem i wdrożeniem nowych i modernizowanych elementów Systemu RZIIP AKO.
3. Za monitorowanie i planowanie pojemności Systemu RZIIP AKO odpowiedzialny jest Główny ASI.
4. Przed dokonaniem odbioru nowych lub modernizowanych elementów Systemu RZIIP AKO istotnych z punktu widzenia funkcjonalności, należy ustalić kryteria ich odbioru oraz przeprowadzić testy sprawdzające.
5. Kryteria odbioru modernizacji Systemu RZIIP AKO powinny uwzględniać następujące elementy:
   1) wymagania dotyczące wydajności i pojemności,
   2) wymagania dotyczące wdrożonych zabezpieczeń,
   3) przygotowania procedur zarządzania incydentami zagrażającymi bezpieczeństwu informacji przetwarzanej i gromadzonej w systemie,
   4) szkolenie w obsłudze i użytkowaniu,
   5) optymalne warunki gwarancji i serwisu,
   6) potwierdzenie, że instalacja nowego elementu Systemu RZIIP AKO nie będzie wpływała niekorzystnie na istniejące systemy.
6. Personel dostawców sprzętu i oprogramowania wykonują usługę tylko za zgodą Głównego ASI.

7. Jeśli rodzaj wykonywanych czynności (np. uaktualnienie, poprawienie błędnej lub wadliwie działającej konfiguracji oprogramowania czy sprzętu) wymusza pracę na kontach administracyjnych – usługa winna być nadzorowana przez administratora systemu.

§ 2 – Zasady sporządzania kopii danych.

1. Informacje zabezpiecza się przed utratą lub uszkodzeniem w przypadku awarii zasilania, sprzętu lub sieci poprzez tworzenie kopii zapasowych.
2. Za sporządzanie kopii zapasowych baz i programów (serwerów) odpowiada Główny ASI. Kopie zapasowe sporządzane są zgodnie z opracowanym przez niego harmonogramem.
3. Bazy danych, oprogramowanie oraz konfiguracja systemów operacyjnych powinny być zabezpieczone w postaci kopii bezpieczeństwa lub archiwalnych oraz posiadać oryginalne nośniki instalacyjne.
4. W celu zabezpieczenia danych, należy wykonywać następujące kopie bezpieczeństwa:
   1) kopie bezpieczeństwa danych, które uległy zmianie, nie rzadziej niż raz dziennie;
   2) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania,
   3) przed dokonaniem zmian w programach (np. zmiana wersji),
   4) po każdej istotnej zmianie danych w bazie danych.
5. Oprócz kopii, o których mowa w ust. 3, należy wykonywać kopie archiwalne na żądanie lub w ramach potrzeb.
6. Za wykonanie i zabezpieczenie kopii, określonych w ust. 4 i 5, odpowiedzialny jest Główny ASI.
7. Weryfikacja poprawności wykonania kopii bezpieczeństwa powinna być wykonywana:
   1) Przynajmniej raz w tygodniu – sprawdzenie wykonania kopii,
   2) Przynajmniej raz w miesiącu – sprawdzenie danych zawartych w kopii.
8. Kopie bezpieczeństwa należy:
   1) wykonywać w taki sposób, aby była dostępna minimum jedna, wcześniej zrobiona kopia bezpieczeństwa,
   2) przechowywać poza miejscem przechowywania danych źródłowych, których kopia bezpieczeństwa była wykonywana.
9. Kopie archiwalne należy:
   1) wykonać w co najmniej dwóch egzemplarzach każda, przy czym przynajmniej jedną na nośniku wymiennym,

2) przechowywać w dwóch różnych urządzeniach i miejscach innych niż te, w którym eksploatowane zbiory przechowywane są na bieżąco.

10. Wykonaną kopię bezpieczeństwa należy przechowywać minimum do momentu wykonania następnej kopii bezpieczeństwa.
11. Nośniki komputerowe, na których znajdują się kopie bezpieczeństwa i archiwalne, powinny być oznaczone w sposób trwały, jednoznaczny i czytelny i zaewidencjonowane w rejestrze zgodnym z załącznikiem nr ADM-04.
12. Kopie archiwalne należy: okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania, bezzwłocznie usuwać po ustaniu ich użyteczności.
13. Ważne dane winny być przechowywane wyłącznie na serwerze Systemu RZIIP AKO. Dopuszcza się przechowywanie ważnych danych lokalnie na komputerze, o ile dane te podlegają cyklicznemu procesowi wykonywania kopii bezpieczeństwa.
14. O trybie zabezpieczenia danych decyduje Główny ASI.
15. Okres przechowywania kopii, powinien wynikać z rodzaju zarchiwizowanych danych oraz być zgodny z przepisami wewnętrznymi JST AKO dotyczącymi archiwizowania.

§ 3 – Monitoring systemu.

1. Główny ASI monitoruje wykorzystanie zasobów sprzętowych przez System RZIIP AKO oraz parametry pracy. Do podstawowych elementów, które są monitorowane należą:
   1) wykorzystanie pamięci masowych;
   2) wykorzystanie pamięci operacyjnych;
   3) przepustowość kart sieciowych;
   4) ruch sieciowy;
   5) obciążenie procesorów;
   6) uwierzytelnienia w systemie;
   7) próby zdalnego dostępu do usług, portów i zasobów;
   8) automatycznie wyzwalane procesy systemów operacyjnych;
   9) dostęp do Internetu z sieci lokalnej.
2. System RZIIP AKO posiada włączone logowanie zdarzeń związanych z bezpieczeństwem umożliwiające identyfikację źródła zagrożenia. Pliki w których przechowywane są zebrane logi podlegają archiwizacji.

3. System tworzenia logów oraz proces ich archiwizacji i przechowywania chroni zapisy przed edycją i nieautoryzowanym dostępem.
4. Główny ASI jest obowiązany wykrywać wszelkie podatności Systemu RZIIP AKO na zagrożenia związane z bezpieczeństwem informacji.
5. Dla poszczególnych systemów powinny zostać ustalone priorytety w zakresie kolejności działań w zakresie wykrywania podatności, systemy o wysokim ryzyku powinny być rozpatrywane jako pierwsze.
6. Główny ASI prowadzi wykaz, zgodny z załącznikiem nr ADM-15, zawierający zestawienie połączeń VPN sieci RZIIP AKO.
7. Każde zdarzenie zagrażające bezpieczeństwu danych lub każde zdarzenie, które spowodowało naruszenie ochrony danych, winno zostać pisemnie udokumentowane przez Głównego ASI poprzez sporządzenie przez niego stosownej notatki oraz umieszczenie w Rejestrze incydentów – załącznik nr ADM-06.

§ 4 – Ewidencja sprzętu i oprogramowania.

1. Główny ASI prowadzi ewidencję sprzętu i oprogramowania Systemu RZIIP AKO.
2. Co najmniej raz na cztery lata dokonywana jest inwentaryzacja sprzętu i oprogramowania w formie spisu z natury. Sprzęt i oprogramowanie może być objęte inwentaryzacją roczną.
3. Nośniki instalacyjne oprogramowania znajdują się na zabezpieczonym hasłem zasobie sieciowym lub w zamkniętej szafie w obszarze podwyższonego bezpieczeństwa, do którego ma dostęp jedynie Główny ASI. Programów nie można kopiować, wypożyczać lub przekazywać osobom trzecim w żadnej formie. Dotyczy to również kodów aktywacyjnych produktów.

§ 5 – Polityka wprowadzania zmian.

1. Przy wprowadzaniu zmian w Systemie RZIIP AKO bierze się pod uwagę aspekt bezpieczeństwa informacji.
2. Decyzja o zmianie podejmowana lub akceptowana jest przez Głównego ASI.
3. Wprowadza się trzy typy zmian:
   1) prosta;
   2) standardowa;

3) awaryjna.

4. Zmiana prosta charakteryzuje się brakiem spadku poziomu bezpieczeństwa teleinformatycznego usług. Zmiany tej nie poddaje się testom. Do zmian prostych zalicza się m. in.:
   1) rutynową kolejną instalację tego samego oprogramowania w tej samej wersji w systemie operacyjnym o tych samych parametrach;
   2) wymianę stacji roboczej na inną, skonfigurowaną w ten sam sposób.
5. Zmiana standardowa charakteryzuje się ingerencją w konfigurację Systemu RZIIP AKO. Może mieć wpływ na obniżenie poziomu świadczonych usługi oraz ich bezpieczeństwo teleinformatyczne. Każda tego typu zmiana powinna być wcześniej poddana testom w środowisku testowym. Do zmian standardowych zalicza się m. in.:
   1) instalację nowego systemu operacyjnego lub oprogramowania na serwerach RZIIP AKO;
   2) aktualizację systemu operacyjnego lub oprogramowania na serwerach RZIIP AKO.
6. Zmiana awaryjna to zmiana zainicjowana przez incydent. Zmianę wykonuje się jak najszybciej w celu przywrócenia poziomu usług.
7. Wszelkie nowo instalowane oprogramowanie musi pochodzić z zaufanego źródła. W pakietach oprogramowania nie należy dokonywać żadnych zmian.

§ 6 – Kontrola sprzętu komputerowego i oprogramowania.

1. Za przeprowadzanie kontroli sprzętu komputerowego i oprogramowania Systemu RZIIP AKO w Urzędzie Miasta Kalisza odpowiada Główny ASI.
2. Za wykonywanie przeglądów i konserwacje sprzętu komputerowego, Systemu RZIIP AKO oraz nośników danych odpowiada Główny ASI.
3. Główny ASI prowadzi wykaz, zgodny z załącznikiem nr ADM-02, zawierający zestawienie oprogramowania i licencji zakupionego w ramach projektu RZIIP AKO.
4. Główny ASI prowadzi wykaz, zgodny z załącznikiem nr ADM-03, zawierający zestawienie sprzętu zakupionego w ramach projektu RZIIP AKO.
5. Główny ASI przeprowadza okresowo kontrolę:
   1) stanu serwerowni, klimatyzacji itp. – Załącznik nr ADM-08;
   2) działania serwerów oraz maszyn wirtualnych – Załącznik nr ADM-09;

3) logów systemowych, zarówno systemów operacyjnych, usług jak i oprogramowania RZIIP AKO – Załącznik nr ADM-10;
4) logowań udanych i nieudanych do systemu RZIIP AKO – Załącznik nr ADM-11;
5) zasileń systemu oraz replikacji danych pomiędzy serwerami – Załącznik nr ADM-12;
6) aktualności systemów operacyjnych, oprogramowania RZIIP AKO, oprogramowania usług, oprogramowania sprzętu – Załącznik nr ADM-13;
7) działania zasilania awaryjnego (UPS) – Załącznik nr ADM-14;
8) połączeń sieci wirtualnych (VPN) – Załącznik nr ADM-16;
9) poprawności wykonania kopii bezpieczeństwa lub archiwalnej – Załącznik nr ADM-17.

6. Każde przeprowadzenie kontroli musi być udokumentowane w rejestrze zgodnym z podanym wzorem.
7. Każde wejście do serwerowni Systemu RZIIP AKO, znajdującej się w Urzędzie Miasta Kalisza należy potwierdzić w odpowiednim rejestrze „wejść do serwerowni" – załącznik nr ADM-07.

§ 7 – Wykonywania przeglądów i konserwacji.

1. Wszelkie prace konserwacyjne i naprawcze sprzętu RZIIP AKO oraz uaktualnienia lub naprawy Systemu RZIIP AKO, wykonywane przez firmę zewnętrzną, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy JST AKO, a tymże podmiotem, z uwzględnieniem klauzuli dotyczącej ochrony przez Zleceniobiorcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi.
2. Prace, o których mowa w ust. 1, winny zostać odnotowane w rejestrze wykonanych usług lub napraw dla sprzętu RZIIP AKO lub oprogramowania RZIIP AKO – załączniki nr od ADM-18 do ADM-21 prowadzonym przez Głównego ASI.
3. W przypadku naprawy sprzętu komputerowego w serwisie zewnętrznym ważne dane należy zabezpieczyć (zarchiwizować) oraz o ile to możliwe usunąć z nośników informacji.

§ 8 – Przechowywanie haseł.

1. Hasła służące do administrowania Systemem RZIIP AKO powinny być spisane oraz umieszczone w zamkniętych kopertach, oddzielnych dla każdego podsystemu lub programu, w miejscu uniemożliwiającym dostęp do nich osób nieupoważnionych, chroniącym przed utratą lub

zniszczeniem oraz gwarantującym ich odczytanie upoważnionemu użytkownikowi, a także kierownikowi właściwej jednostki organizacyjnej w przypadkach nadzwyczajnych. Zarejestrowane hasła, powinny posiadać adnotację o dacie ich wprowadzenia. Do kopert należy prowadzić rejestr zgodny ze wzorem – załącznik nr ADM-22.

2. Otwieranie kopert z hasłami administracyjnymi powinno odbywać się tylko w uzasadnionych przypadkach, lub w razie nieobecności Głównych ASI. Użycie hasła administracyjnego systemu może się odbyć tylko za zgodą przełożonego właściciela hasła oraz odpowiednio udokumentowane, zgodnie ze wzorem – załącznik nr ADM-23.
3. Po każdej zmianie hasła w systemie Główny ASI tworzy nową kopertę z hasłem, a poprzednia jest niszczona bez otwierania.

§ 9 – Okresowa analiza ryzyka.

1. Analiza ryzyka jest składową procesu podejmowania decyzji, ułatwiającą kierującym podejmowanie świadomych i właściwych wyborów, ustalenia priorytetów działań oraz rozpoznawania alternatywnych kierunków działań w przypadku zaistniałych zagrożeń, zdarzeń i sytuacji kryzysowych.
2. Analizę ryzyka należy prowadzić w sposób ciągły, nie rzadziej niż raz do roku.
3. Analizę ryzyka Systemu RZIIP AKO przeprowadza Inspektor Ochrony Danych Urzędu Miasta Kalisza.
4. W analizie szacowania ryzyka określa się parametry charakterystyczne dla wystąpienia ryzyka:
   1) prawdopodobieństwo wystąpienia ryzyka (oznaczenie P),
   2) podatność systemu na wystąpienie ryzyka (oznaczenie W),
   3) ocenę skutku zaistnienia ryzyka (oznaczenie S).
5. Ocenę parametrów prawdopodobieństwa, podatności i skutku dokonuje się w oparciu o 3-punktową skalę wartości: małe (1 pkt.), średnie (2 pkt.), wysokie (3 pkt).
6. Wartość ryzyka dla Systemu RZIIP AKO wylicza się mnożąc wartości punktowe.
7. Wyniki szacowania ryzyka należy umieścić w Rejestrze ryzyk – załącznik nr ADM-05.
8. Po oszacowaniu ryzyka należy określić metody postępowania z ryzykiem zgodnie z poniższą zasadą:
   1) Wartość ryzyka do 10 pkt. – Akceptacja ryzyka,
   2) Wartość ryzyka do 11-17 pkt. – Redukowanie ryzyka,

3) Wartość ryzyka do 18-27 pkt. – Przeniesienie ryzyka.

9. Metody postępowania z ryzykiem:
   1) Akceptacja ryzyka – brak działań i akceptacja na skutki wystąpienia ryzyka;
   2) Redukowanie ryzyka – działania zmierzające do znacznego ograniczenia lub całkowitego wyeliminowania skutków wystąpienia ryzyka, są to działania o charakterze infrastrukturalnym, proceduralnym lub jedno i drugie;
   3) Przeniesienie ryzyka – działania polegające na wykorzystaniu mechanizmów prawnych lub działań o charakterze organizacyjnym, przenoszących ryzyko na inny podmiot.

Załączniki.

Załącznik	***Nazwa załącznika***	***Występowanie w Polityce***
UŻYTKOWNICY		
1	Oświadczenie pracownika o zapoznaniu z Polityką Bezpieczeństwa RZIIP AKO	I. §9.1.
2	Wykaz grup uprawnień i uprawnień do Systemu RZIIP AKO	I. §12.7.
3	Procedura utworzenia nowego użytkownika w Systemie RZIIP AKO	I. §12.3. II. §1.3.
4	Procedura modyfikacji użytkownika oraz jego uprawnień w Systemie RZIIP AKO	I. §6.4. II. §1.4.
5	Procedura cofnięcia uprawnień użytkownika do Systemu RZIIP AKO	I. §6.1. II. §1.4.
6	Wniosek utworzenia, modyfikacji lub cofnięcia uprawnień użytkownika Systemu RZIIP AKO	I. §6.1. I. §6.2. I. §12.5.
7	Wniosek utworzenia, modyfikacji lub cofnięcia uprawnień administratora lokalnego Systemu RZIIP AKO	II. §1.3.
8	Rejestr administratorów Systemu RZIIP AKO	II. §1.5.
9	Rejestr użytkowników Systemu RZIIP AKO	II. §10.13.
ADMINISTRATOR GŁÓWNY		
ADM-01	Procedury administracyjne realizowane przez Administratora głównego Systemu RZIIP AKO	-
ADM-02	Rejestr oprogramowania i licencji Systemu RZIIP AKO	III. §6.3.
ADM-03	Rejestr sprzętu RZIIP AKO	III. §6.4.
ADM-04	Rejestr nośników danych Systemu RZIIP AKO	III. §2.11.
ADM-05	Rejestr ryzyk Systemu RZIIP AKO	III. §9.7.
ADM-06	Rejestr incydentów Systemu RZIIP AKO	III. §3.8.
ADM-07	Rejestr wejść do serwerowni głównej Systemu RZIIP AKO	III. §6.7.
ADM-08	Rejestr przeglądu serwerowni głównej Systemu RZIIP AKO	III. §6.5.1)
ADM-09	Rejestr przeglądu serwerów głównych Systemu RZIIP AKO	III. §6.5.2)
ADM-10	Rejestr przeglądu logów Systemu RZIIP AKO	III. §6.5.3)
ADM-11	Rejestr przeglądu logowań udanych i nieudanych Systemu RZIIP AKO	III. §6.5.4)

Załącznik	***Nazwa załącznika***	***Występowanie w Polityce***
ADM-12	Rejestr przeglądu zasileń danych oraz replikacji danych Systemu RZIIP AKO	III. §6.5.5)
ADM-13	Rejestr przeglądu aktualności Systemu RZIIP AKO	III. §6.5.6)
ADM-14	Rejestr testów UPS serwerowni głównej RZIIP AKO	III. §6.5.7)
ADM-15	Rejestr połączeń VPN Systemu RZIIP AKO	III. §3.6
ADM-16	Rejestr testów VPN Systemu RZIIP AKO	III. §6.5.8)
ADM-17	Rejestr przeglądu poprawności wykonania kopii bezpieczeństwa lub archiwalnej Systemu RZIIP AKO	III. §6.5.9)
ADM-18	Rejestr napraw sprzętu RZIIP AKO	III. §7.2.
ADM-19	Rejestr usług dodatkowych dla sprzętu RZIIP AKO	III. §7.2.
ADM-20	Rejestr napraw oprogramowania Systemu RZIIP AKO	III. §7.2.
ADM-21	Rejestr usług dodatkowych Systemu RZIIP AKO	III. §7.2.
ADM-22	Rejestr kopert z hasłami	III. §8.1.
ADM-23	Rejestr otwarcia kopert z hasłami	III. §8.2.

Załącznik nr 1 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Oświadczenie pracownika

.....

(nazwisko i imię)

.....

(nazwa komórki organizacyjnej)

.....

(nazwa jednostki organizacyjnej)

OŚWIADCZENIE

Niniejszym oświadczam, że:

1. zapoznałam(-em) się z obowiązującymi przepisami dotyczącymi bezpieczeństwa Systemu RZIIP AKO, oraz Polityką Bezpieczeństwa Systemu RZIIP AKO,
2. zobowiązuję się do ich przestrzegania.

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _

(miejscowość, data)

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _

(czytelny podpis)

Załącznik nr 2 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Wykaz grup uprawnień i uprawnień do Systemu RZIIP AKO

Grupy uprawnień Systemu RZIIP AKO

Grupa	Opis	Grupa	Opis
JST_BL	Dostęp do danych z Gminy Blizanów	JST_CK	Dostęp do danych z Gminy Ceków Kolonia
JST_GO	Dostęp do danych z Gminy Gołuchów	JST_GW	Dostęp do danych z Gminy Godziesze Wielkie
JST_KA	Dostęp do danych z Miasta Kalisz	JST_KO	Dostęp do danych z Gminy Koźminek
JST_LI	Dostęp do danych z Gminy Lisków	JST_MY	Dostęp do danych z Gminy Mycielin
JST_NS	Dostęp do danych z Gminy Nowe Skalmierzyce	JST_OD	Dostęp do danych z Gminy Odolanów
JST_OG	Dostęp do danych z Gminy Ostrów Wielkopolski	JST_OM	Dostęp do danych z Miasta Ostrów Wielkopolski
JST_OP	Dostęp do danych z Gminy Opatówek	JST_OS	Dostęp do danych ze Starostwa Powiatowego w Ostrowie Wielkopolskim
JST_PK	Dostęp do danych ze Starostwa Powiatowego w Kaliszu	JST_PR	Dostęp do danych z Gminy Przygodzice
JST_PS	Dostęp do danych ze Starostwa Powiatowego w Pleszewie	JST_RA	Dostęp do danych z Gminy Raszków
JST_SI	Dostęp do danych z Gminy Sieroszewice	JST_SO	Dostęp do danych z Gminy Sośnie
JST_ST	Dostęp do danych z Gminy Stawiszyn	JST_SZ	Dostęp do danych z Gminy Szczytniki
JST_ZE	Dostęp do danych z Gminy Żelazków		

Załącznik nr 2 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Wykaz grup uprawnień i uprawnień do Systemu RZIIP AKO

Uprawnienia Systemu RZIIP AKO

Lp	ID uprawnienia	Opis uprawnienia
1.	**_ZALOGOWANY**	Uprawnienia do wewnętrznego Systemu RZIIP AKO.
2.	**_ELUD**	Uprawnienie dostępu do danych Ewidencji Ludności.
3.	**_EGIB***	Uprawnienie dostępu do danych i raportów Ewidencji Gruntów i Budynków.*
4.	**_RCN***	Uprawnienie dostępu do danych i raportów Rejestru Cen Nieruchomości.*
5.	**_ZK**	Uprawnienie dostępu do danych, ich edycji i raportów danych z grupy Zarządzania Kryzysowego.
6.	**_EDIOM_O**	Uprawnienie dostępu oraz odczytu danych z systemu Ewidencja Dróg i Obiektów Mostowych.
7.	**_EDIOM_E**	Uprawnienie edycji danych w systemie Ewidencja Dróg i Obiektów Mostowych.
8.	**_WYDARZENIA**	Uprawnienie dostępu do danych, ich edycji i raportów danych z grupy Wydarzenia.
9.	**_OGLOSZENIA**	Uprawnienie dostępu do danych, ich edycji i raportów danych z grupy Ogłoszenia.
10.	**_MIENIE**	Uprawnienie dostępu do danych, ich edycji i raportów danych z grupy Gospodarka Mieniem.
* wymaga akceptacji przez właściwego Starostę.		

Uprawnienia Administratora lokalnego Systemu RZIIP AKO

Grupa	Opis	Grupa	Opis
JST_BL_ADMIN	Uprawnienia dla administratora Gminy Blizanów	JST_CK_ADMIN	Uprawnienia dla administratora Gminy Ceków Kolonia
JST_GO_ADMIN	Uprawnienia dla administratora Gminy Gołuchów	JST_GW_ADMIN	Uprawnienia dla administratora Gminy Godziesze Wielkie
JST_KA_ADMIN	Uprawnienia dla administratora Miasta Kalisza	JST_KO_ADMIN	Uprawnienia dla administratora Gminy Koźminek
JST_LI_ADMIN	Uprawnienia dla administratora Gminy Lisków	JST_MY_ADMIN	Uprawnienia dla administratora Gminy Mycielin
JST_NS_ADMIN	Uprawnienia dla administratora Gminy Nowe Skalmierzyce	JST_OD_ADMIN	Uprawnienia dla administratora Gminy Odolanów
JST_OG_ADMIN	Uprawnienia dla administratora Gminy Ostrów Wielkopolski	JST_OM_ADMIN	Uprawnienia dla administratora Miasta Ostrów Wielkopolski
JST_OP_ADMIN	Uprawnienia dla administratora Gminy Opatówek	JST_OS_ADMIN	Uprawnienia dla administratora Starostwa Powiatowego w Ostrowie Wielkopolskim
JST_PK_ADMIN	Uprawnienia dla administratora Starostwa Powiatowego w Kaliszu	JST_PR_ADMIN	Uprawnienia dla administratora Gminy Przygodzice
JST_PS_ADMIN	Uprawnienia dla administratora Starostwa Powiatowego w Pleszewie	JST_RA_ADMIN	Uprawnienia dla administratora Gminy Raszków
JST_SI_ADMIN	Uprawnienia dla administratora Gminy Sieroszewice	JST_SO_ADMIN	Uprawnienia dla administratora Gminy Sośnie
JST_ST_ADMIN	Uprawnienia dla administratora Gminy Stawiszyn	JST_SZ_ADMIN	Uprawnienia dla administratora Gminy Szczytniki
JST_ZE_ADMIN	Uprawnienia dla administratora Gminy Żelazków		

Załącznik nr 3 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Procedura utworzenia uprawnień użytkownika / administratora lokalnego Systemu RZIIP AKO

§ 1.

Procedura obiegu dokumentu, celem utworzenia uprawnień użytkownika / administratora lokalnego Systemu RZIIP AKO.

1. Podstawą utworzenia nowego użytkownika i nadania mu uprawnień, jest upoważnienie do przetwarzania danych.
2. Potrzeba dostępu do danych powinna być uzasadniona zakresem realizowanych przez pracownika zadań.
3. Nadanie uprawnień do Systemu RZIIP AKO wymaga złożenia przez pracownika stosownego oświadczenia (Załącznik nr 1 Polityki bezpieczeństwa Systemu RZIIP AKO).
4. Nadanie uprawnień do Systemu RZIIP AKO dla nowego użytkownika, nadane jest na pisemny wniosek przełożonego pracownika na złożonym na formularzu „wniosek utworzenia, modyfikacji lub cofnięcia uprawnień użytkownika Systemu RZIIP AKO" (Załącznik nr 6 Polityki bezpieczeństwa Systemu RZIIP AKO).
5. Nadanie uprawnień dla lokalnego administratora Systemu RZIIP AKO należy złożyć na formularzu „wniosek utworzenia lub cofnięcia uprawnień administratora lokalnego Systemu RZIIP AKO" (Załącznik nr 7 Polityki bezpieczeństwa Systemu RZIIP AKO).
6. Wniosek utworzenia uprawnień użytkownika wypełniany jest w dwóch kopiach. Jedna dla administratora lokalnego Systemu RZIIP AKO, druga dla użytkownika.
7. Wniosek utworzenia uprawnień administratora lokalnego wypełniany jest w trzech kopiach. Jedna dla administratora głównego Systemu RZIIP AKO, druga dla administratora lokalnego, trzeci do dokumentacji jednostki administratora lokalnego.
8. Uprawnienie musi zostać zaakceptowane przez Inspektora Ochrony Danych danej jednostki, a następnie kierownika danej jednostki.
9. W przypadku pracowników zatrudnionych na stanowisku kierownika komórki organizacyjnej lub samodzielnym stanowisku pracy wniosek podpisuje nadzorujący to stanowisko kierownik jednostki lub jego zastępca, sekretarz jednostki, skarbnik jednostki.
10. Wnioskowanie o uprawnienia dostępu do Ewidencji Gruntów i Budynków oraz Rejestru Cen Nieruchomości wymaga akceptacji przez właściwego Starostę. W przypadku Urzędu Miasta Kalisza zgodę na dostęp do tych baz danych w imieniu kierownika jednostki powiatu wyraża Geodeta Powiatowy – Naczelnik Wydziału Geodezji i Kartografii urzędu.
11. Osoby wymienione w ust.8-10 mogą zmienić zakres wnioskowanych uprawnień.
12. Zatwierdzenie wniosku utworzenia uprawnień administratora lokalnego JST AKO wykonywane jest w imieniu Prezydenta Miasta Kalisza przez Naczelnika Wydziału Geodezji i Kartografii lub jego zastępcę.
13. Zatwierdzony wniosek utworzenia uprawnień użytkownika stanowi podstawę dla administratora lokalnego danej jednostki do utworzenia nowego użytkownika i nadania mu odpowiednich uprawnień w Systemie RZIIP AKO.
14. Zatwierdzony wniosek utworzenia uprawnień administratora lokalnego JST AKO stanowi podstawę dla administratora głównego Systemu RZIIP AKO do utworzenia nowego administratora i nadania mu odpowiednich uprawnień w Systemie RZIIP AKO.
15. Kopia zaakceptowanych formularzy zostaje przekazana w formie elektronicznej (dokument zeskanowany) do administratora głównego Systemu RZIIP AKO.

16. Administrator główny Systemu RZIIP AKO może zastąpić administratora lokalnego Systemu RZIIP AKO w zakresie wprowadzania nowego użytkownika na wniosek kierownika danej jednostki lub administratora lokalnego Systemu RZIIP AKO.

§ 2.

Instrukcja obiegu dokumentu, celem utworzenia uprawnień użytkownika / administratora lokalnego Systemu RZIIP AKO.

1. Wniosek należy wydrukować w 2 egzemplarzach (użytkownik Systemu RZIIP AKO) lub 3 egzemplarzach (administrator lokalny Systemu RZIIP AKO).
2. Wniosek o nadanie uprawnień administratora lokalnego posiada wyłącznie jedną stronę, czynności wypełniania tabeli uprawnień nie dotyczą go.
3. Użytkownik lub przełożony użytkownika dla którego składany jest wniosek o nadanie uprawnień, wypełnia **CZĘŚĆ A** wniosku oraz w tabeli uprawnień użytkownika wypełnia pola „**Wnioskowane**".
4. **CZĘŚĆ B** - Akceptacja wniosku wymaga podpisów przez:
   1) Przełożonego użytkownika/administratora lokalnego dla którego składany jest wniosek.
   2) Inspektora Ochrony Danych Osobowych JST AKO w której pracuje użytkownik/administrator lokalny dla którego składany jest wniosek.
   3) Kierownika JST AKO w której pracuje użytkownik/administrator lokalny dla którego składany jest wniosek.
5. Jeśli wniosek dotyczy utworzenia uprawnień użytkownika, akceptacji wymaga również tabela z uprawnieniami użytkownika oraz wypełnienia pól „**Przyznane**" przez Kierownika JST AKO z wyłączeniem uprawnień _EGIB oraz _RCN (o ile były wnioskowane takie uprawnienia).
6. W przypadku składania wniosku o nadanie uprawnień _EGIB, _RCN lub administratora lokalnego, w **CZĘŚCI C**, dla:
   1) użytkownika, który będzie miał dostęp do danych rozszerzonych Ewidencji Gruntów i Budynków lub Rejestru Cen Nieruchomości – wymagany jest podpis kierownika jednostki powiatu, którego dane dotyczą lub upoważnionego przez niego pracownika. Tj. w przypadku gmin z powiatu kaliskiego – Starostwa Powiatowego w Kaliszu, w przypadku gmin z powiatu ostrowskiego – Starostwa Powiatowego w Ostrowie Wielkopolskim, w przypadku gminy Gołuchów – Starostwa Powiatowego w Pleszewie.
      W przypadku Urzędu Miasta Kalisza zgodę na dostęp do tych baz danych w imieniu kierownika jednostki powiatu wyraża Geodeta Powiatowy – Naczelnik Wydziału Geodezji i Kartografii urzędu.
   2) Administratora lokalnego – potwierdzenie wniosku o nadanie uprawnień przez kierownika jednostki powiatu, którego dane dotyczą lub upoważnionego przez niego pracownika oraz Naczelnika Wydziału Geodezji i Kartografii Urzędu Miasta w Kaliszu lub jego zastępcy.
7. Jeśli wniosek dotyczy utworzenia uprawnień użytkownika w zakresie uprawnień _EGIB oraz _RCN, wypełnienia pól „**Przyznane**" w tabeli uprawnień przez kierownika jednostki powiatu, którego dane dotyczą lub upoważnionego przez niego pracownika. W przypadku Urzędu Miasta Kalisza zgodę na dostęp do tych baz danych w imieniu kierownika jednostki powiatu wyraża Geodeta Powiatowy – Naczelnik Wydziału Geodezji i Kartografii urzędu.
8. **CZĘŚĆ D** wypełnia Administrator lokalny lub główny w zakresie pól identyfikator, grupa JST oraz podpis administratora. Wprowadza odpowiednie uprawnienia do systemu, wraz z zaznaczeniem w tabeli uprawnień odpowiednich pól „**Nadane**".
9. **CZĘŚĆ D** wniosku o nadanie uprawnień administratora lokalnego wypełnia administrator główny Systemu RZIIP AKO.
10. Nomenklatura nadawania identyfikatorów użytkowników w systemie:

```
dwie litery określające jednostkę + '_' + imię + '.' + nazwisko
```

11. Użytkownik lub administrator lokalny, dla którego składany jest wniosek, potwierdzają zapoznanie się otrzymanymi uprawnieniami poprzez złożenie podpisu w **CZĘŚCI D.**
12. Zeskanowany wniosek wraz z zeskanowany oświadczeniem należy przesłać drogą elektroniczną administratorowi głównemu Systemu RZIIP AKO.

Załącznik nr 4 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Procedura modyfikacji dostępu do danych dla użytkownika Systemu RZIIP AKO

§ 1.

Procedura obiegu dokumentu, celem modyfikacji dostępu do danych dla użytkownika Systemu RZIIP AKO.

1. Podstawą modyfikacji dostępu do danych dla użytkownika, jest upoważnienie do przetwarzania danych.
2. Potrzeba modyfikacji dostępu do danych powinna być uzasadniona zakresem realizowanych przez pracownika zadań.
3. Modyfikacja uprawnień do Systemu RZIIP AKO dla użytkownika, wykonywana jest na pisemny wniosek przełożonego pracownika na złożonym na formularzu „wniosek utworzenia, modyfikacji lub cofnięcia uprawnień użytkownika Systemu RZIIP AKO" (Załącznik nr 6 Polityki bezpieczeństwa Systemu RZIIP AKO).
4. Wniosek modyfikacji dostępu do danych dla użytkownika wypełniany jest w dwóch kopiach. Jedna dla administratora lokalnego Systemu RZIIP AKO, druga dla użytkownika.
5. Uprawnienie musi zostać zaakceptowane przez Inspektora Ochrony Danych danej jednostki, a następnie kierownika danej jednostki.
6. W przypadku pracowników zatrudnionych na stanowisku kierownika komórki organizacyjnej lub samodzielnym stanowisku pracy wniosek podpisuje nadzorujący to stanowisko kierownik jednostki lub jego zastępca, sekretarz jednostki, skarbnik jednostki.
7. Wnioskowanie o uprawnienia dostępu do Ewidencji Gruntów i Budynków oraz Rejestru Cen Nieruchomości wymaga akceptacji przez właściwego kierownika jednostki. W przypadku Urzędu Miasta Kalisza zgodę na dostęp do tych baz danych w imieniu kierownika jednostki powiatu wyraża Geodeta Powiatowy – Naczelnik Wydziału Geodezji i Kartografii urzędu.
8. Osoby wymienione w ust.8-10 mogą zmienić zakres wnioskowanych uprawnień.
9. Zatwierdzony wniosek modyfikacji uprawnień użytkownika stanowi podstawę dla administratora lokalnego danej jednostki do utworzenia nowego użytkownika i nadania mu odpowiednich uprawnień w Systemie RZIIP AKO.
10. Kopia zaakceptowanych formularzy zostaje przekazana w formie elektronicznej (dokument zeskanowany) do administratora głównego Systemu RZIIP AKO.
11. Administrator główny Systemu RZIIP AKO może zastąpić administratora lokalnego Systemu RZIIP AKO w zakresie wprowadzania nowego użytkownika na wniosek kierownika danej jednostki lub administratora lokalnego Systemu RZIIP AKO.

§ 2.

Instrukcja obiegu dokumentu, celem modyfikacji dostępu uprawnień użytkownika Systemu RZIIP AKO.

1. Wniosek należy wydrukować w 2 egzemplarzach.
2. Użytkownik lub przełożony użytkownika dla którego składany jest wniosek o modyfikacje uprawnień, wypełnia **CZĘŚĆ A** wniosku oraz w tabeli uprawnień użytkownika wypełnia pola „**Wnioskowane**".
3. **CZĘŚĆ B** - Akceptacja wniosku wymaga podpisów przez:
   1) Przełożonego użytkownika dla którego składany jest wniosek.
   2) Inspektora Ochrony Danych Osobowych JST AKO w której pracuje użytkownik dla którego składany jest wniosek.
   3) Kierownika JST AKO w której pracuje użytkownik dla którego składany jest wniosek.
4. Akceptacji wymaga również tabela z uprawnieniami użytkownika oraz wypełnienia pól „**Przyznane**" przez Kierownika JST AKO z wyłączeniem uprawnień _EGIB oraz _RCN (o ile były wnioskowane takie uprawnienia).
5. W **CZĘŚCI C**, dla użytkownika, który będzie miał dostęp do danych rozszerzonych Ewidencji Gruntów i Budynków lub Rejestru Cen Nieruchomości – wymagany jest podpis kierownika jednostki powiatu, którego dane dotyczą lub upoważnionego przez niego pracownika. Tj. w przypadku gmin z powiatu kaliskiego – Starostwa Powiatowego w Kaliszu, w przypadku gmin z powiatu ostrowskiego – Starostwa Powiatowego w Ostrowie Wielkopolskim, w przypadku gminy Gołuchów – Starostwa Powiatowego w Pleszewie. W przypadku Urzędu Miasta Kalisza zgodę na dostęp do tych baz danych w imieniu kierownika jednostki powiatu wyraża Geodeta Powiatowy – Naczelnik Wydziału Geodezji i Kartografii urzędu.
6. Jeśli wniosek dotyczy utworzenia uprawnień użytkownika w zakresie uprawnień _EGIB oraz _RCN, wypełnienia pól „**Przyznane**" w tabeli uprawnień przez kierownika jednostki powiatu, którego dane dotyczą lub upoważnionego przez niego pracownika. W przypadku Urzędu Miasta Kalisza zgodę na dostęp do tych baz danych w imieniu kierownika jednostki powiatu wyraża Geodeta Powiatowy – Naczelnik Wydziału Geodezji i Kartografii urzędu.
7. **CZĘŚĆ D** wypełnia Administrator lokalny lub główny w zakresie pól identyfikator, grupa JST oraz podpis administratora. Wprowadza odpowiednie uprawnienia do systemu, wraz z zaznaczeniem w tabeli uprawnień odpowiednich pól „**Nadane**".
8. Użytkownik, dla którego składany jest wniosek, potwierdzają zapoznanie się otrzymanymi uprawnieniami poprzez złożenie podpisu w **CZĘŚCI D.**
9. Zeskanowany wniosek należy przesłać drogą elektroniczną administratorowi głównemu Systemu RZIIP AKO.

Załącznik nr 5 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Procedura cofnięcia uprawnień użytkownika / administratora lokalnego Systemu RZIIP AKO

§ 1.

Procedura obiegu dokumentu, celem cofnięcia uprawnień użytkownika / administratora lokalnego Systemu RZIIP AKO.

1. Cofnięcie uprawnień użytkownika lub administratora Systemu RZIIP AKO wiąże się z blokadą dostępu do Systemu RZIIP AKO.
2. Częściowe cofnięcie uprawnień dla użytkownika powinno być składane poprzez modyfikację uprawnień na złożonym formularzu „wniosek utworzenia, modyfikacji lub cofnięcia uprawnień użytkownika Systemu RZIIP AKO" (Załącznik nr 6 Polityki bezpieczeństwa Systemu RZIIP AKO).
3. Cofnięcie uprawnień do Systemu RZIIP AKO dla użytkownika, wykonywane jest na pisemny wniosek przełożonego pracownika na złożonym formularzu „wniosek utworzenia, modyfikacji lub cofnięcia uprawnień użytkownika Systemu RZIIP AKO" (Załącznik nr 6 Polityki bezpieczeństwa Systemu RZIIP AKO).
4. Cofnięcie uprawnień administratora lokalnego Systemu RZIIP AKO należy złożyć na formularzu „wniosek utworzenia lub cofnięcia uprawnień administratora lokalnego Systemu RZIIP AKO" (Załącznik nr 7 Polityki bezpieczeństwa Systemu RZIIP AKO).
5. Wniosek cofnięcia uprawnień dla użytkownika wypełniany jest w dwóch kopiach. Jedna dla administratora lokalnego Systemu RZIIP AKO, druga dla użytkownika.
6. Wniosek cofnięcia uprawnień dla administratora lokalnego wypełniany jest w trzech kopiach. Jedna dla administratora głównego Systemu RZIIP AKO, druga dla administratora lokalnego, trzeci do dokumentacji jednostki administratora lokalnego.
7. W przypadku pracowników zatrudnionych na stanowisku kierownika komórki organizacyjnej lub samodzielnym stanowisku pracy wniosek podpisuje nadzorujący to stanowisko kierownik jednostki lub jego zastępca, sekretarz jednostki, skarbnik jednostki.
8. Zatwierdzony wniosek cofnięcia uprawnień dla użytkownika stanowi podstawę dla administratora lokalnego Systemu RZIIP AKO danej jednostki do cofnięcia uprawnień dla użytkownika w Systemie RZIIP AKO.
9. Zatwierdzony wniosek cofnięcia uprawnień dla administratora lokalnego stanowi podstawę dla administratora głównego Systemu RZIIP AKO do cofnięcia uprawnień dla użytkownika w Systemie RZIIP AKO.
10. Kopia zaakceptowanych formularzy zostaje przekazana w formie elektronicznej (dokument zeskanowany) do administratora głównego Systemu RZIIP AKO.
11. Administrator główny Systemu RZIIP AKO może zastąpić administratora lokalnego Systemu RZIIP AKO w zakresie cofnięcia uprawnień użytkownika na wniosek kierownika danej jednostki lub administratora lokalnego Systemu RZIIP AKO.

§ 2.

Instrukcja obiegu dokumentu, celem cofnięcia uprawnień użytkownika / administratora lokalnego Systemu RZIIP AKO.

1. Wniosek należy wydrukować w 2 egzemplarzach (użytkownik Systemu RZIIP AKO) lub 3 egzemplarzach (administrator lokalny Systemu RZIIP AKO).
2. Wniosek o cofnięcie uprawnień należy wypełnić wyłącznie w **CZĘŚCI A**, oraz w **CZĘŚCI B**.
3. Użytkownik lub przełożony użytkownika dla którego składany jest wniosek o cofnięcie uprawnień, wypełnia **CZĘŚĆ A** wniosku.
4. **CZĘŚĆ B** - Akceptacja wniosku wymaga podpisów przez:
   a) Przełożonego użytkownika/administratora lokalnego dla którego składany jest wniosek o cofnięcie uprawnień.
   b) Kierownika JST AKO w której pracuje użytkownik/administrator lokalny dla którego składany jest wniosek.
5. **CZĘŚĆ C** - *nie wymaga wypełnienia.*
6. **CZĘŚĆ D** wypełnia Administrator lokalny lub główny w zakresie pól identyfikator, grupa JST oraz podpis administratora. Cofa odpowiednie uprawnienia dla użytkownika do systemu Systemu RZIIP AKO.
7. **CZĘŚĆ D** wniosku o cofnięcie uprawnień administratora lokalnego wypełnia administrator główny Systemu RZIIP AKO.
8. Użytkownik lub administrator lokalny, dla którego składany jest wniosek, potwierdzają zapoznanie się cofniętymi uprawnieniami poprzez złożenie podpisu w **CZĘŚCI D.**
9. Zeskanowany wniosek wraz z zeskanowany oświadczeniem należy przesłać drogą elektroniczną administratorowi głównemu Systemu RZIIP AKO.

Załącznik nr 6 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Wniosek utworzenia, modyfikacji lub cofnięcia uprawnień użytkownika systemu RZIIP AKO

CZĘŚĆ A

(nazwisko i imię) .....

(nazwa komórki organizacyjnej) .....

(nr upoważnienia do przetwarzania danych) .....

(nazwa jednostki organizacyjnej) .....

(e-mail) .....

□ utworzenie uprawnień użytkownika
□ modyfikacja uprawnień użytkownika
□ usunięcie uprawnień użytkownika

(modyfikacja) .....

CZĘŚĆ B

(podpis przełożonego) .....

(podpis IOD) .....

(podpis kierownika jednostki) .....

CZĘŚĆ C

Potwierdzam przyznanie wnioskowanego uprawnienia dostępu do danych

Uzupełniane w przypadku wniosku o nadanie uprawnień _EGIB, _RCN

(data / podpis kierownika jednostki powiatu, którego dane dotyczą) .....

Uprawnienie obowiązuje z chwilą nadania do czasu pisemnego cofnięcia.

Uprawnienie upoważnia do dostępu do danych wyłącznie dostępnych dla danej jednostki.

CZĘŚĆ D

Potwierdzam nadanie / modyfikację / cofnięcie uprawnienia do Systemu RZIIP AKO:

(identyfikator) .....

(grupa JST) .....

(data / podpis administratora lokalnego lub głównego) .....

(data / podpis pracownika) .....

Załącznik nr 6 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Wniosek utworzenia, modyfikacji lub cofnięcia uprawnień użytkownika systemu RZIIP AKO

Lp	ID uprawnienia	Opis uprawnienia	Wnioskowane	Przyznane	Nadane
1.	_ZALOGOWANY	Uprawnienia do wewnętrznego Systemu RZIIP AKO.			
2.	_ELUD	Uprawnienie dostępu do danych Ewidencji Ludności.			
3.	_EGIB*	Uprawnienie dostępu do danych i raportów Ewidencji Gruntów i Budynków.*			
4.	_RCN*	Uprawnienie dostępu do danych i raportów Rejestru Cen Nieruchomości.*			
5.	_ZK	Uprawnienie dostępu do danych, ich edycji i raportów danych z grupy Zarządzania Kryzysowego.			
6.	_EDIOM_O	Uprawnienie dostępu oraz odczytu danych z systemu Ewidencja Dróg i Obiektów Mostowych.			
7.	_EDIOM_E	Uprawnienie edycji danych w systemie Ewidencja Dróg i Obiektów Mostowych.			
8.	_WYDARZENIA	Uprawnienie dostępu do danych, ich edycji i raportów danych z grupy Wydarzenia.			
9.	_OGLOSZENIA	Uprawnienie dostępu do danych, ich edycji i raportów danych z grupy Ogłoszenia.			
10.	_MIENIE	Uprawnienie dostępu do danych, ich edycji i raportów danych z grupy Gospodarka Mieniem.			
* wymaga akceptacji kierownika jednostki powiatu, którego dane dotyczą.					

.....
(nazwisko i imię)

.....
(nazwa jednostki organizacyjnej / nazwa komórki organizacyjnej)

.....
(podpis przełożonego)

.....
(podpis kierownika jednostki)

.....
(podpis kierownika jednostki powiatu, którego dane dotyczą)

Załącznik nr 7 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Wniosek utworzenia lub cofnięcia uprawnień administratora lokalnego systemu RZIIP AKO

AKO

CZĘŚĆ A

(nazwisko i imię) .....

(nazwa komórki organizacyjnej) .....

(nr upoważnienia do przetwarzania danych) .....

(nazwa jednostki organizacyjnej) .....

□ utworzenie uprawnień administratora
□ cofnięcie uprawnień administratora

(e-mail) .....

(modyfikacja) .....

CZĘŚĆ B

(podpis przełożonego) .....

(podpis IOD) .....

(podpis kierownika jednostki) .....

CZĘŚĆ C

Potwierdzam przyznanie wnioskowanego uprawnienia dostępu do danych

(data / podpis kierownika jednostki powiatu, którego dane dotyczą) .....

(data / podpis Naczelnika Wydziału Geodezji i Kartografii UM Kalisz) .....

Uprawnienie obowiązuje z chwilą nadania do czasu pisemnego cofnięcia.

Uprawnienie upoważnia wyłącznie do administracji systemem RZIIP AKO w zakresie nadawania uprawnień, tworzenia lub modyfikacji użytkowników lub danych dostępnych dla danej jednostki.

CZĘŚĆ D

Potwierdzam utworzenie/cofnięcie uprawnienia do Systemu RZIIP AKO:

(identyfikator) .....

(grupa JST) .....

(data / podpis administratora głównego) .....

(data / podpis pracownika) .....

Załącznik nr 8 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr administratorów Systemu RZIIP AKO

(karta) (stan na dzień)

Lp	JST	Nazwisko, Imię	Dane kontaktowe e-mail / telefon	Uwagi

Załącznik nr 9 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr użytkowników Systemu RZIIP AKO

(karta) (stan na dzień)

Lp	JST	Nazwisko, Imię	Dane kontaktowe e-mail / telefon	Grupy uprawnień

Procedury administracyjne Systemu RZIIP AKO

§ 1. – Procedura przeglądu serwerowni

1. Z powodu przechowywania danych osobowych i innych, które nie powinny być upublicznione, procedurę może wykonywać wyłącznie upoważniona osoba.
2. Wejście do serwerowni osób nieupoważnionych odbywać się może wyłącznie w asyście osób upoważnionych.
3. Przegląd musi być wykonywany codziennie, wraz z odpowiednią adnotacją w Rejestrze przeglądu serwerowni (Załącznik nr ADM-08 Polityki bezpieczeństwa Systemu RZIIP AKO).
4. Przegląd serwerowni głównej obejmuje przegląd organoleptyczny stanu pomieszczenia oraz sprzętu w nim się znajdującego:
   1) Weryfikacja działania klimatyzatora oraz chłodzenia serwerowni, czy temperatura na czujniku odpowiada, lub jest niższa niż ustawiona na jednostce wewnętrznej klimatyzatora.
   2) Weryfikacja czujników alarmowych.
   3) Weryfikacja zamknięcia okien i opuszczonych rolet.
   4) Weryfikacja działania serwerów, sprawdzenie czy nie pojawiły się błędy dysków.
   5) Weryfikacja działania UPSów.
   6) Weryfikacja działania Switchy.
   7) Weryfikacja zamknięcia szaf i innych urządzeń znajdujących się w pomieszczeniu.

§ 2. – Procedura przeglądu statusu serwerów i QNAP

1. Z powodu przechowywania danych osobowych i innych, które nie powinny być upublicznione, procedurę może wykonywać wyłącznie upoważniona osoba.
2. Wejście do serwerowni osób nieupoważnionych odbywać się może wyłącznie w asyście osób upoważnionych.
3. Przegląd musi być wykonywany codziennie, wraz z odpowiednią adnotacją w Rejestrze przeglądu serwerów głównych (Załącznik nr ADM-09 Polityki bezpieczeństwa Systemu RZIIP AKO).
4. Przegląd statusu serwerów i QNAP obejmuje połączenie z aplikacją ZABBIX lub Webmin w przypadku serwerów, lub serwerem QNAP i zweryfikowaniem poprawności działania:
   1) Połączenie się z aplikacją ZABBIX lub Webmin.
   2) Sprawdzenie poprawności działania serwerów oraz QNAP.
   3) W przypadku wątpliwości działania poszczególnych serwerów i aplikacji, wymagane sprawdzenie logów do nich przypisanych (§ 3. – Procedura przeglądu logów).

§ 3. – Procedura przeglądu logów

1. Z powodu przechowywania danych osobowych i innych, które nie powinny być upublicznione, procedurę może wykonywać wyłącznie upoważniona osoba.
2. Częstotliwość przeglądu jest uzależniona od rodzaju logu i nie może być ściśle określona. Należy przyjąć, że ważne logi, m.in. geoserver, wymagają przeglądu przynajmniej raz na tydzień. Inne nie rzadziej niż raz w miesiącu.
3. Ważność i częstotliwość przeglądu określa administrator Systemu RZIIP AKO.
4. W uzasadnionych przypadkach częstotliwość przeglądu może zostać zwiększona. Również w przypadku wystąpienia błędów lub awarii.

5. Potwierdzenie wykonania przeglądu logów musi zostać poświadczone, wraz z odpowiednią adnotacją w Rejestrze przeglądu logów (Załącznik nr ADM-10 Polityki bezpieczeństwa Systemu RZIIP AKO).
6. Przegląd logów obejmuje pobranie plików, ich przeczytanie i sprawdzenie, czy pojawiają się niepokojące zapisy, informujące o nieprzewidzianym działaniu Systemu RZIIP AKO lub występowaniem błędów. Przegląd logów obejmuje logi działania aplikacji, a także statusu serwerów i ich części składowych.
   1) Połączenie się z aplikacją ZABBIX.
   2) Weryfikacja połączeń ze wszystkimi serwerami wirtualnymi.
   3) Monitorowanie zasobów systemowych.
   4) Sprawdzenie innych mierników celem weryfikacji poprawności działania.
   5) Połączenie się z aplikacją Webmin.
   6) Weryfikacja poprawności działania Systemu RZIIP AKO.
   7) W przypadku wątpliwości działania poszczególnych serwerów i aplikacji, wymagane sprawdzenie logów do nich przypisanych.

§ 4. – Procedura przeglądu logowań

1. Z powodu przechowywania danych osobowych i innych, które nie powinny być upublicznione, procedurę może wykonywać wyłącznie upoważniona osoba.
2. Częstotliwość przeglądu jest zmienna. Ważność i częstotliwość przeglądu określa administrator Systemu RZIIP AKO.
3. W uzasadnionych przypadkach częstotliwość przeglądu może zostać zwiększona. Również w przypadku wystąpienia błędów lub awarii, a także zgłoszeń użytkowników o niemożliwości zalogowania.
4. Potwierdzenie wykonania przeglądu musi zostać poświadczone, wraz z odpowiednią adnotacją w Rejestrze przeglądu logowań (Załącznik nr ADM-11 Polityki bezpieczeństwa Systemu RZIIP AKO).
5. Przegląd logowań obejmuje sprawdzenie wystąpienia problemów z logowaniami dla określonych użytkowników, a także prób zalogowania do systemu poprzez inne narzędzia służące do ataków i włamań metodą bruteforce:
   1) Połączenie się z aplikacją.
   2) Weryfikacja listy logów od czasu ostatniej weryfikacji.

§ 5. – Procedura przeglądu zasileń i replikacji

1. Z powodu przechowywania danych osobowych i innych, które nie powinny być upublicznione, procedurę może wykonywać wyłącznie upoważniona osoba.
2. Częstotliwość przeglądu jest zmienna. Ważność i częstotliwość przeglądu określa administrator Systemu RZIIP AKO.
3. W uzasadnionych przypadkach częstotliwość przeglądu może zostać zwiększona. Również w przypadku wystąpienia błędów lub awarii, a także zgłoszeń użytkowników o niemożliwości zalogowania.
4. Potwierdzenie wykonania przeglądu musi zostać poświadczone, wraz z odpowiednią adnotacją w Rejestrze przeglądu zasileń i replikacji (Załącznik nr ADM-12 Polityki bezpieczeństwa Systemu RZIIP AKO).
5. Przegląd zasileń obejmuje sprawdzenie wystąpienia problemów z zasilaniami z zewnętrznych systemów lub innych baz, także geokodowania. Przegląd replikacji obejmuje sprawdzenie wystąpienia problemów z replikacją danych z serwera wewnętrznego do zewnętrznego.

6. Zasilanie systemu RZIIP AKO odbywa się poprzez następujące kanały:
   1) szyny usług na serwerach importujących dane oraz serwerze centralnym,
   2) wprowadzanie i edycja danych w oprogramowaniu dziedzinowym GeoAra,
   3) import danych do oprogramowania dziedzinowego,
   4) podłączanie źródeł zewnętrznych za pomocą serwera danych przestrzennych (pliki lub usługi sieciowe).

§ 6. – Procedura przeglądu aktualności Systemu RZIIP AKO

1. Z powodu przechowywania danych osobowych i innych, które nie powinny być upublicznione, procedurę może wykonywać wyłącznie upoważniona osoba.
2. Częstotliwość przeglądu jest zmienna. Ważność i częstotliwość przeglądu określa administrator Systemu RZIIP AKO.
3. W uzasadnionych przypadkach częstotliwość przeglądu może zostać zwiększona. Również w przypadku wystąpienia błędów lub awarii, a także zgłoszeń użytkowników o niemożliwości zalogowania.
4. Potwierdzenie wykonania przeglądu musi zostać poświadczone, wraz z odpowiednią adnotacją w Rejestrze przeglądu aktualności (Załącznik nr ADM-13 Polityki bezpieczeństwa Systemu RZIIP AKO).
5. Przegląd aktualności obejmuje sprawdzenie aktualności systemów operacyjnych, ich komponentów, sterowników, firmware oraz BIOS.

§ 7. – Procedura testów UPS serwerowni głównej

1. Procedurę może wykonywać wyłącznie upoważniona osoba, posiadająca niezbędne uprawnienia do wykonania tej czynności.
2. Procedurę wykonuje administrator Systemu RZIIP AKO w serwerowni Systemu RZIIP AKO.
3. Częstotliwość przeglądu jest zmienna. Ważność i częstotliwość przeglądu określa administrator Systemu RZIIP AKO, jednakże nie rzadziej niż raz na miesiąc.
4. W uzasadnionych przypadkach częstotliwość przeglądu może zostać zwiększona.
5. Potwierdzenie wykonania przeglądu musi zostać poświadczone, wraz z odpowiednią adnotacją w Rejestrze testów UPS (Załącznik nr ADM-14 Polityki bezpieczeństwa Systemu RZIIP AKO).
6. Test UPS obejmuje połączenie się z serwerami głównymi poprzez kartę IPMI i weryfikowanie poprzez ręczne wyłączenie UPS z gniazda zasilającego, czy UPS oraz system poprawnie reagują. Dodatkowym testem jest weryfikacja połączenia sieciowego UPS:
   1) Połączenie z głównymi serwerami poprzez kartę IPMI.
   2) Uruchomienie narzędzia PING na każdy UPS.
   3) Pojedyncze wypięcie kabla sieciowego z UPS (kolejność od góry do dołu).
   4) Weryfikacja na serwerze braku połączenia z danym UPS.
   5) Zakończenie połączenia, lub kontynuowanie testu podtrzymywania bateryjnego.
   6) Uruchomienie połączenia z każdym głównym serwerem, poprzez kartę IPMI.
   7) Pojedyncze wypięcie kabla zasilającego dany UPS.
   8) Weryfikacja na serwerze komunikatu o zaniku zasilania.
   9) Zakończenie testów

§ 8. – Procedura testów połączeń VPN

1. Procedurę może wykonywać wyłącznie upoważniona osoba, posiadająca niezbędne uprawnienia do wykonania tej czynności.
2. Procedurę wykonuje administrator Systemu RZIIP AKO w serwerowni Systemu RZIIP AKO.
3. Częstotliwość przeglądu jest zmienna. Ważność i częstotliwość przeglądu określa administrator Systemu RZIIP AKO, jednakże nie rzadziej niż raz na tydzień.
4. W uzasadnionych przypadkach częstotliwość przeglądu może zostać zwiększona.
5. Potwierdzenie wykonania przeglądu musi zostać poświadczone, wraz z odpowiednią adnotacją w Rejestrze testów VPN (Załącznik nr ADM-16 Polityki bezpieczeństwa Systemu RZIIP AKO).
6. Test połączenia VPN obejmuje połączenie się z aplikacją ZABBIX i weryfikację połączenia z serwerem importującym. W przypadku braku widoczności serwera wymagane wykorzystanie narzędzia PING:
   1) Połączenie z aplikacją ZABBIX.
   2) Weryfikacja połączeń z serwerami importującymi.
   3) W przypadku jednostkowego braku połączenia, wykorzystanie narzędzia PING.
   4) Jeśli w aplikacji ZABBIX widnieje połączenie, test jest zakończony, nie trzeba wykorzystywać narzędzia PING.
   5) Zakończenie testów.

§ 9. – Procedura rozpoczęcia, zawieszenia i zakończenia pracy w Systemie RZIIP AKO

1. Procedurę może wykonywać wyłącznie upoważniona osoba, posiadająca niezbędne uprawnienia do wykonania tej czynności.
2. Procedurę wykonuje administrator Systemu RZIIP AKO.
3. W celu uruchomienia i rozpoczęcia pracy administrator powinien wybrać odpowiednią opcję umożliwiającą logowanie do Systemu, zalogować się do Systemu poprzez wskazanie loginu oraz poufnego i aktualnego hasła.
4. Administrator podczas logowania do systemu nie może ujawniać hasła osobom trzecim, w tym innym administratorom oraz pozostawiać zapisanego hasła w pobliżu stanowiska pracy i innych pracowników.
5. Administrator zobligowany jest do skutecznego wylogowania się z systemu za każdym razem, gdy zamierza opuścić stanowisko pracy, niezależnie od tego na jak długo ma zamiar odejść od stanowiska pracy. Wylogowanie następuje poprzez wybranie w Systemie opcji wylogowania.

§ 10. – Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Procedurę może wykonywać wyłącznie upoważniona osoba, posiadająca niezbędne uprawnienia do wykonania tej czynności.
2. Procedurę wykonuje administrator Systemu RZIIP AKO.
3. Kopie zapasowe zbiorów danych wykonuje Administrator na żądanie lub w ustalonym harmonogramie, zgodnie z potrzebami przechowywania wybranego zbioru danych, na wyznaczone urządzenie NAS, korzystając z wbudowanych w to urządzenie narzędzi oraz mechanizmów udostępnianych natywnie przez systemy operacyjne serwerów, na których znajdują się dane do zachowania w postaci kopii zapasowej.

4. Administrator główny nadzoruje poprawność procesu tworzenia i przechowywania kopii zapasowych, w tym celu dokonuje cyklicznego przeglądu tworzenia kopii zapasowych.
5. Częstotliwość przeglądu jest zmienna. Ważność i częstotliwość przeglądu określa administrator Systemu RZIIP AKO, jednakże nie rzadziej niż raz na miesiąc.
6. W uzasadnionych przypadkach częstotliwość przeglądu może zostać zwiększona.
7. Potwierdzenie wykonania przeglądu musi zostać poświadczone, wraz z odpowiednią adnotacją w Rejestrze przeglądu kopii (Załącznik nr ADM-17 Polityki bezpieczeństwa Systemu RZIIP AKO).

§ 11. – Procedura przywracania systemu lub jego części z kopii zapasowej

1. Procedurę może wykonywać wyłącznie upoważniona osoba, posiadająca niezbędne uprawnienia do wykonania tej czynności.
2. Procedurę wykonuje Administrator główny Systemu RZIIP AKO.
3. Administrator główny Systemu RZIIP AKO wykorzystuje skrypty i/lub usługi przygotowane specjalnie do tego celu, czerpiąc z magazynu kopii zapasowych znajdującego się na wyznaczonym urządzeniu NAS. Administrator główny nadzoruje poprawność przywracania systemu z kopii zapasowych.

Załącznik nr ADM-02 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr oprogramowania i licencji Systemu RZIIP AKO

AKO

.....

(karta)

Lp	JST	Data	Nazwa oprogramowania	Typ licencji	Licencja ważna do	Podpis administratora RZIIP AKO	Uwagi

Załącznik nr ADM do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr sprzętu Systemu RZIIP AKO

AKO

.....

(karta)

Lp	JST	Data	Nazwa sprzętu	Typ sprzętu	Numer seryjny / produkcyjny	Podpis administratora RZIIP AKO	Uwagi

Załącznik nr ADM-04 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr nośników danych Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Data	Nazwa sprzętu	Numer seryjny / produkcyjny	Rodzaj przechowywanych danych	Podpis administratora RZIIP AKO	Uwagi

Załącznik nr ADM-05 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr ryzyk Systemu RZIIP AKO

AKO

LP	Zdarzenie	Skutek	P	W	S	Reakcja na ryzyko	Działanie	Właściciel ryzyka
1.	Nieuprawniony dostęp do Systemu RZIIP	Utrata poufności, integralności, dostępności informacji						
2.	Nieuprawniony dostęp do informacji w Systemie RZIIP	Utrata poufności informacji						
3.	Awaria lub brak ciągłości działania Systemu RZIIP	Brak dostępności informacji, utrudnienia w pracy Urzędu						
4.	Wprowadzenie do Systemu RZIIP złośliwego kodu wirusa	Utrata, zniszczenie lub udostępnienie informacji, niewłaściwa praca Systemu RZIIP						
5.	Nieuprawnione udostępnienie lub zniszczenie informacji	Utrata, zniszczenie lub udostępnienie informacji w całości lub części						
6.	Nieświadome udostępnienie lub zniszczenie informacji	Utrata, zniszczenie lub udostępnienie informacji w całości lub części						
7.	Celowe udostępnienie	Nieuprawniony dostęp do informacji						
8.	Utrata danych w wyniku pożaru	Zniszczenie infrastruktury Systemu RZIIP, utrata danych						
9.	Utrata danych w wyniku powodzi lub zalania	Zniszczenie infrastruktury Systemu RZIIP, utrata danych						

Rejestr ryzyk Systemu RZIIP AKO

AKO

10.	Utrata danych w wyniku zwarcia w instalacji elektrycznej lub uderzenia pioruna	Zniszczenie infrastruktury Systemu RZIIP, utrata danych						
11.	Uszkodzenie nośnika danych	Ograniczenie dostępu do danych, utrata części danych lub całości danych						
12.	Utrata kopii zapasowych	Niemożliwość odtworzenia części lub całości danych						
13.	Awaria łączy telekomunikacyjnych	Ograniczenie dostępu do części danych lub całości danych						
14.	Awaria prądu	Ograniczenie dostępu do części danych lub całości danych, możliwa utrata całości lub części danych						

Załącznik nr ADM-06 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr incydentów Systemu RZIIP AKO

AKO

LP	Czas i miejsce	Incydent	Przyczyny	Zakres i skutki incydentu	Konsekwencje	Środki zaradcze	Osoby odpowiedzialne za ryzyko	Naprawa / odtworzenie

Załącznik nr ADM-07 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr wejść do serwerowni głównej Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Data	Osoba	Czynność

Załącznik nr ADM-08 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr przeglądu serwerowni głównej Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Data	Osoba	Uwagi	Podpis

Załącznik nr ADM-09 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr przeglądu serwerów głównych Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Data	Osoba	Serwery	QNAP	Uwagi	Podpis

Załącznik nr ADM-10 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr przeglądu logów Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Data	Osoba	Zabbix	Serwery wirtualne	Dysk/ Procesor/ RAM	Webmin	Logi	Uwagi	Podpis

Załącznik nr ADM-11 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr przeglądu logowań udanych i nieudanych do Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Data	Osoba	Uwagi	Podpis

Załącznik nr ADM-12 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr przeglądu zasileń danych oraz replikacji danych Systemu RZIIP AKO

.....

(karta)

Lp	Data	Osoba	EGIB i RCN	ELUD	Inne Systemy dziedzinowe	Uwagi	Podpis

Załącznik nr ADM-13 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr przeglądu aktualności Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Data	Osoba	Systemy Operacyjne	Oprogramowanie RZIIP AKO	Oprogramowanie usług RZIIP AKO	Oprogramowanie sprzętu	Uwagi	Podpis

Załącznik nr ADM-14 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr testów UPS serwerowni głównej Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Data wykonania testu	Osoba	PING	Zasilenie	Uwagi	Podpis

Załącznik nr ADM-15 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr połączeń VPN Systemu RZIIP AKO

AKO

.....

(karta) (stan na dzień)

Lp	JST	Uwagi

Załącznik nr ADM-16 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr testów VPN Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Data wykonania testu	Osoba	ZABBIX	PING	Uwagi	Podpis

Załącznik nr ADM-17 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr przeglądu poprawności wykonania kopii bezpieczeństwa lub archiwalnej Systemu RZIIP AKO

.....

(karta)

Lp	Data przeglądu	Osoba	Uwagi	Podpis

Załącznik nr ADM-18 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr napraw sprzętu Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Urządzenie techniczne / nr seryjny / opis awarii	Data awarii / zgłoszenia	Data odbioru / zwrotu	Dokument / Uwagi	Podpis

Załącznik nr ADM-19 do „Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr usług dodatkowych dla sprzętu Systemu RZIIP AKO

AKO

.....

(karta)

Lp	Urządzenie techniczne / nr seryjny / opis	Data zgłoszenia / koszt	Data odbioru / zwrotu	Dokument / Uwagi	Podpis

Załącznik nr ADM-20 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr napraw oprogramowania Systemu RZIIP AKO

AKO

.....

(karta)

Lp	System / oprogramowanie / opis awarii	Data awarii / zgłoszenia	Data naprawy	Dokument / Uwagi	Podpis

Załącznik nr ADM-21 do ,,Polityki bezpieczeństwa Systemu RZIIP AKO"

Rejestr usług dodatkowych Systemu RZIIP AKO

AKO

.....

(karta)

Lp	System / oprogramowanie / opis	Data zgłoszenia / koszt	Data odbioru	Dokument / Uwagi	Podpis

Rejestr kopert z hasłami do Systemu RZIIP AKO

.....

(karta)

Lp	Data	Ilość kopert	Uwagi	Podpis

Rejestr otwarcia kopert z hasłami do Systemu RZIIP AKO

.....

(karta)

Lp	Data	Przyczyna otwarcia koperty	Podpis osoby 01	Podpis osoby 02