**Województwo Świętokrzyskie** *Załącznik* ***nr 1*** *do OPZ*

**2601 Powiat Buski**

**2602 Powiat Jędrzejowski**

**2604 Powiat Kielecki**

**2608 Powiat Pińczowski**

**PLAN CIĄGŁOŚCI DZIAŁANIA**

**dla powiatów:**

**buskiego, jędrzejowskiego, kieleckiego i pińczowskiego**

**na wypadek awarii Geoportalu   
będącego bezpośrednim produktem Projektu e-GEODEZJA**

**Spis treści**

[I. Informacje wstępne 3](#_Toc4516455)

[II. Analiza lokalizacji pomieszczenia serwerowni, zabezpieczenia, kopie zapasowe………….…4](#_Toc4516456)

III. Analiza istniejących zagrożeń, działania na wypadek awarii……………………………….…………..10

1. **Informacje wstępne**
   1. Poniższy Plan ciągłości działania, nazywany dalej Planem, powstał w celu udokumentowania procedur u wszystkich partnerów realizujących w Porozumienie Projekt e-GEODEZJA, które po wystąpieniu zakłócenia w działaniu rozbudowanego Geoportalu, mają wspierać organizację w reagowaniu, uzyskiwaniu sprawności, oraz odbudowie działania na wcześniej zdefiniowanym poziomie operacyjnym (Norma ISO 22301).
   2. Oprócz identyfikacji i zastosowania środków bezpieczeństwa, takich jak np:

* urządzenia do podtrzymywania zasilania (UPS),
* detektory dymu i ognia,
* czujniki wody w pomieszczeniach ze sprzętem komputerowym,
* instalacje przeciwpożarowe,
* regularnie wykonywane i właściwie przechowywane kopie zapasowe,
* odpowiednio przygotowane miejsca (poza siedzibą starostwa) służące do przechowywania kopii zapasowych, danych w postaci nieelektronicznej oraz dokumentacji systemu, w Planie powinna zostać opisana strategia przywracania działania Geoportalu w oparciu o podobny sprzęt wykorzystywany przez poszczególnych partnerów.

1.2. W Planie określono między innymi:

* minimalną częstość wykonywania kopii zapasowych,
* zasoby danych, z których kopie należy wykonać,
* format, w jakim będą zapisywane nośniki z danymi zapasowymi.
  1. Geoportal, czyli System, który jest bezpośrednim produktem Projektu, powinien cechować się dostępnością co najmniej na poziomie 99,9% ( co oznacza brak dostępności maks. 8 godz. 45 min w roku) dla powiatów realizujących w partnerstwie Projekt pn. e-GEODEZJA-cyfrowy zasób powiatów: buskiego, jędrzejowskiego, kieleckiego i pińczowskiego; natomiast cały zintegrowany system łącznie z istniejącym już back-officem powinien cechować się dostępnością na poziomie 99% (czyli czasem braku dostępności 3 d 11 h 20 min w skali roku).
  2. W razie potrzeby Partnerzy Projektu zakładają zawarcie odpowiednich umów serwisowych (SLA) zapewniających dostępność całego systemu oraz monitorowanie dostępności w ramach geoportalu (dostępności witryny internetowej) będącej przedmiotem Projektu.

1. **Analiza lokalizacji pomieszczenia serwerowni, zabezpieczenia, kopie zapasowe.**

**2.1. powiat Buski**

**2.1.1. Analiza lokalizacji pomieszczenia serwerowni.**

Serwerownia tutejszego Starostwa usytuowana jest na parterze budynku. Okna w pomieszczeniu zabezpieczone są kratami zarówno wewnętrznymi jak i zewnętrznymi. Przez serwerownię poprowadzone są również piony centralnego ogrzewania co mogłoby spowodować ewentualne zalanie. Grzejnik usytuowany przy oknie jest obecnie wyłączony. Dostęp do pomieszczenia zabezpieczony jest certyfikowanymi drzwiami oraz zamontowano kontrolę dostępu. Serwerownię uzbrojono w czujniki ruchu oraz zadymienia. Ochronę całodobową sprawuje zewnętrzna firma ochroniarska. W pomieszczeniu funkcjonuje system klimatyzacji co pozwala na zabezpieczenie sprzętu przed przegrzaniem. Zamontowano system kontroli temperatury oraz wilgotności, który powiadamia wiadomością e-mail oraz sms Administratora Systemu Informatycznego o przekroczonych stanach granicznych.

**2.1.2. Zabezpieczenia**

W ramach zabezpieczenia Geoportalu, na styku sieci wewnętrznej i zewnętrznej zamontowano firewall w postaci UTM. Serwery, na których zainstalowano Geoportal pracują w wydzielonej strefie sieci (DMZ) bez możliwości ingerencji osób nieuprawnionych z sieci wewnętrznej. Wprowadzono system logów z każdej procedury wykonywanej na Geoportalu.

Sprzęt (serwery, switche, routery, macierze) posiadają zabezpieczenie przez zanikiem napięcia poprzez podłączenie ich do zasilaczy awaryjnych UPS. Usługa monitoringu działania Geoportalu połączona jest z systemem powiadomienia e-mail oraz sms. Na wypadek awarii Administrator Systemu Informatycznego powiadamiany jest w/w sposób i jest w stanie określić poziom awarii usługi oraz systemu operacyjnego.

**2.1.3. Kopie zapasowe**

System Geoportalu podzielony jest na dwa wyodrębnione zasoby, publiczny i niepubliczny. Zasób publiczny udostępniony jest z ograniczonej w dane kopii systemu produkcyjnego, jego ewentualna kompromitacja nie wpłynie na wyciek danych osobowych jak i integralność danych produkcyjnych. Zasób niepubliczny dodatkowo chroniony jest za pomocą certyfikatów SSL dla użytkowników co już na poziomie sieciowym ogranicza dostęp do serwerów geoportalu do osób uprawnionych dla których urząd wydał certyfikaty. Kopia zapasowa systemu oraz baz danych wykonywana jest w systemie dziennym. Obrazy serwerów wykonywane są w interwale tygodniowym. W/w kopie przechowywane są na dedykowanych macierzach dyskowych. System w godzinach nocnych wykonuje backup na macierz umieszczoną w jednym budynku tut. Starostwa. Raz na dobę następuje replikacja danych backupowych na dodatkową macierz usytuowaną w drugiej lokalizacji Starostwa Powiatowego w Busko-Zdroju.

**2.2. powiat Jędrzejowski**

**2.2.1.** **Analiza lokalizacji pomieszczenia serwerowni.**

Serwerownia Wydziału Geodezji, Kartografii i Katastru Starostwa Powiatowego w Jędrzejowie usytuowana jest na I piętrze budynku, zlokalizowanego przy ul. Armii Krajowej 9. Dostęp do pomieszczenia zabezpieczony jest certyfikowanymi drzwiami oraz zamontowano kontrolę dostępu. Serwerownię uzbrojono w czujniki ruchu oraz zadymienia. W pomieszczeniu funkcjonuje system klimatyzacji co pozwala na zabezpieczenie sprzętu przed przegrzaniem. Budynek, w którym mieści się serwerownia jest zabezpieczony alarmem. Przez serwerownię poprowadzone są również piony centralnego ogrzewania co mogłoby spowodować ewentualne zalanie.

Do obsługi informatyczno-programowej wykorzystywany jest serwer Fujitsu Primergy RX2520 M1 Xeon Six-Core E5-2420 v2 2,2GHz 32GB RAM 2x1TB SATA/RAID1, macierz z systemem Windows Serwer 2012 SP2. Serwer jest zabezpieczony poprzez awaryjny zasilacz APC UPS 1000x2 szt.

**2.2.2**. **Zabezpieczenia**

W ramach zabezpieczenia Geoportalu, na styku sieci wewnętrznej i zewnętrznej zamontowano firewall w postaci UTM. Serwery, na których zainstalowano Geoportal pracują w wydzielonej strefie sieci (DMZ) bez możliwości ingerencji osób nieuprawnionych z sieci wewnętrznej. Wprowadzono system logów z każdej procedury wykonywanej na Geoportalu.

Sprzęt (serwery, switche, routery, macierze) posiadają zabezpieczenie przez zanikiem napięcia poprzez podłączenie ich do zasilaczy awaryjnych UPS.

Polityka bezpieczeństwa systemu informatycznego uregulowana została Zarządzeniem Starosty Jędrzejowskiego nr 32/2018 z dnia 5 czerwca 2018r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwa Informacji ( SZBI) w Starostwie Powiatowym w Jędrzejowie oraz w sprawie wprowadzania „ Instrukcji Zarządzania Systemem Informatycznym Starostwa Powiatowego w Jędrzejowie”.

**2.2.3. Kopie zapasowe**

Kopie bezpieczeństwa prowadzonych baz danych wykonywane są codziennie w podziale na dni parzyste i nieparzyste w kasetach streamer. Na kopiach tych przechowywane są dane z dwóch ostatnich dni. Synchronizacja kopii baz danych na serwery zapasowe, kopie w cyklu tygodniowym na urządzenie pamięci znajdujące się poza Starostwem. Wykonywana jest również kopia danych w cyklu miesięcznym na kasety streamer przechowywane przez rok w serwerowni budynku Starostwa Powiatowe w Jędrzejowie, ul. Armii Krajowej 9. Kopie w cyklu półrocznym wykonywane są na przenośnych dyskach zewnętrznych USB, przechowywanych w budynku siedziby Wojewódzkiej Inspekcji geodezyjnej i Kartograficznej w Kielcach.

System Geoportalu podzielony jest na dwa wyodrębnione zasoby, publiczny i niepubliczny. Zasób publiczny udostępniony jest z ograniczonej w dane kopii systemu produkcyjnego, jego ewentualna kompromitacja nie wpłynie na wyciek danych osobowych jak i integralność danych produkcyjnych. Zasób niepubliczny dodatkowo chroniony jest za pomocą certyfikatów SSL dla użytkowników co już na poziomie sieciowym ogranicza dostęp do serwerów geoportalu do osób uprawnionych dla których zostały założone konta dostępu do Geoportalu. Kopia zapasowa systemu oraz baz danych wykonywana jest w systemie dziennym. Obrazy serwerów wykonywane są w interwale tygodniowym. W/w kopie przechowywane są na dedykowanych macierzach dyskowych. System w godzinach nocnych wykonuje backup na macierz umieszczoną w drugiej lokalizacji Starostwa Powiatowego w Jędrzejowie. Raz na dobę następuje replikacja danych backupowych na dodatkową macierz usytuowaną w drugiej lokalizacji Starostwa Powiatowego w Jędrzejowie.

**2.3. powiat Kielecki**

**2.3.1.** **Analiza lokalizacji pomieszczenia serwerowni.**

Serwerowy sprzęt przetwarzający informacje rozlokowany jest w sposób ograniczający dostęp osób postronnych. Wejście do pomieszczenia serwerowni chronione jest poprzez system kontroli dostępu oraz system alarmowy. Dostęp do pomieszczeń serwerowni posiadają pracownicy Zespołu ds. informatyzacji.

Wszystkie serwery oraz komputery w Starostwie wyposażone są w zasilanie awaryjne pochodzące z centralnego UPS’a, który informuje za pomocą wiadomości email o wszelkich zagrożeniach związanych z brakiem zasilania. Wszystkie pomieszczenia biurowe wyposażone s w system kontroli dostępu, a serwerownia także system sygnalizacji napadu i włamania oraz redundantną klimatyzację, której praca wystarcza do zapewnienia właściwych warunków eksploatacji. W serwerowni zainstalowany jest system gaszenia gazem oraz system kontroli temperatury, który po przekroczeniu wartości brzegowych informuje o zdarzeniu za pomocą wiadomości email oraz sms. Dostęp do wszystkich pomieszczeń w Starostwie nadzorowany jest przez System Kontroli Dostępu, zapewniający pełna rozliczalność w zakresie nadawania uprawnień oraz monitorowania osób otwierających pomieszczenia. Budynek wyposażony jest w system oświetlenia awaryjnego oraz awaryjnej łączności w postaci redundantnego łącza radiowego.

Okablowanie sieci komputerowej Starostwa jest rozłożone w torach kablowych w przestrzeni sufitowej oraz w przestrzeni podłogowej w przypadku serwerowni, minimalizujących ryzyko ich przypadkowego uszkodzenia. Punkty dystrybucyjne znajdują się w odosobnionych, specjalnie do tego celu przeznaczonych, klimatyzowanych pomieszczeniach, w których znajdują się szafy krosowe. Istnieje 10 takich punktów dystrybucyjnych, po 2 na każdą kondygnację. System okablowania sieci komputerowej został zaprojektowany w taki sposób, że okablowanie pionowe prowadzone jest medium miedzianym, nieprzekraczającym długości 90 m od gniazda abonenckiego do punktu dystrybucyjnego. Okablowanie pionowe zostało zaprojektowane w oparciu o medium światłowodowe.

Sieć lokalna Starostwa Powiatowego w Kielcach zbudowana jest z okablowania strukturalnego kategorii 7Aw oparciu o system wkładek wymiennych ACO. Przyjęto generalna zasadę, że okablowanie poziome prowadzone jest za pomocą medium miedzianego, a okablowanie pionowe wykonano za pomocą medium światłowodowego, łączącego 10 Pietrowych punktów dystrybucyjnych z serwerownią, w której zlokalizowany jest rdzeń sieci w postaci dwóch 10-gigabajtowych switchy „datacenter” typu Top-Of-Rack. Każdy punkt dystrybucyjny PPD posiada dwa „up-linki” 10-gigabajtow do serwerowni, po jednym dla każdego z rdzeni, zachowując zasadę redundancji łącza. Rozwiązanie to pozwala zachować pełną funkcjonalność sieci w przypadku awarii jednego z rdzeni, lub któregokolwiek z połączeń pomiędzy PPD a serwerownią.

Z punktu widzenia rozdziału logicznego sieci, wyodrębniono w Starostwie wirtualne sieci lokalne VLAN w celu odseparowania różnych grup urządzeń oraz użytkowników. Zarządzaniem tą częścią sieci kieruje system NAC (Network Access Control), który na podstawie różnych polityk potrafi przypisać urządzenia do konkretnego VLAN-u.

System serwerów oparty jest w głównej mierze na środowisku wirtualnym, zbudowanym przy wykorzystaniu oprogramowania wirtualizacyjnego VMWare oraz Hyper-V. Większość serwerów wykorzystywanych w Starostwie zainstalowanych jest w postaci maszyn wirtualnych zlokalizowanych na jednym z 6-ciu hostów serwera kasetowego „blade”. Jeżeli producent oprogramowania, dla którego instalowany jest serwer nie zaleca inaczej, nowe oraz istniejące serwery migrowane są w miarę możliwości do środowiska wirtualnego. Pozwala to na bezpieczne i efektywne zarzadzanie nimi, wykonywanie kopii bezpieczeństwa oraz ich odtwarzanie w szybki sposób.

W celu zapewnienia integralności wprowadzonych lub modyfikowanych danych w bazach Starostwa, wszystkie serwery i stacje komputerowe synchronizują swoje zegary z kontrolerem domeny.

Dostęp do sieci Internet kontrolowany jest poprzez zainstalowany w siec LAN UTM- Fortigate stanowiący firewall brzegowy oraz router.

Zgodnie z zaleceniami Rozporządzenia o Ochronie Danych Osobowych RODO została wykupiona usługa kolokacji urządzeń serwerowych. W przypadku awarii krytycznej serwerowni znajdującej się na poziomie -1 Starostwo Powiatowe w Kielcach zachowa ciągłość działania, gdyż role serwerowni przejma kolokowanie urządzenia.

Zespól ds. informatyzacji wdrożył darmowy system ZABBIX-oprogramowanie klasy enterprise do obsługi problemów infrastruktury informatycznej. Aplikacja służy do zbierania, analizowania i wizualizacji danych. Oprogramowanie potrafi również wykryć wszelkie anomalie w naszej infrastrukturze i powiadomić o tym administratora.

ZABBIX monitoruje cały system a w przypadku awarii, sprzętowej bądź programowej powiadamia pracowników działu IT poprzez wiadomości e-mail oraz SMS o zaistniałym problemie. W newralgicznych pomieszczeniach tj. serwerownia, centralny US, PPD na każdym poziomie wdrożono system monitorowania warunków środowiskowych, który w przypadku przekroczenia wartości progowej temperatury (niedziałająca klimatyzacja, brak prądu) powiadamia o tym fakcie pracowników ZI. System skorelowany jest z systemem SMS i ZABBIX.

Sprzęt serwerowy na którym działają systemy geodezyjne jest podłączony do dwóch redundantnych UPS-ów. Dodatkowo UPS-y są podłączone do Centralnego UPS-a. W przypadku braku zasilania budynku automatycznie uruchamia się generator prądu, który podłączony jest do Centralnego UPS-a.

W serwerowni zamontowane są cztery klimatyzatory utrzymujące odpowiednia temperaturę w pomieszczeniu. Urządzenia te są podłaodłączone pod centralny UPS, więc w przypadku awarii zasilania będzie utrzymywana odpowiednia temperatura w serwerowni. W serwerowni zamontowany jest system kontroli temperatury, który po przekroczeniu wartości brzegowych informuje o zdarzeniu za pomocą wiadomości e-mail oraz sms..

Głównym łączem jest medium światłowodowe o przepustowości symetrycznej 2 Gbit/s. Ponadto w celu zapewnienia ciągłości działania urzędu oraz nieprzerwanego działania usługi Geoportal, Starostwo posiada redundancje łącza internetowego. Zapasowym łączem, które w przypadku awarii łącza podstawowego automatycznie przełączy się jako aktywne jest łącze radiowe o przepustowości symetrycznej 2—Mbit/s.

**2.3.2.** **Zabezpieczenia**

W ramach zabezpieczenia Geoportalu, na styku sieci wewnętrznej i zewnętrznej zamontowano firewall w postaci UTM. Serwery, na których zainstalowano Geoportal pracują w wydzielonej strefie sieci (DMZ) bez możliwości ingerencji osób nieuprawnionych z sieci wewnętrznej. Wprowadzono system logów z każdej procedury wykonywanej na Geoportalu.

Sprzęt (serwery, switche, routery, macierze) posiadają zabezpieczenie przez zanikiem napięcia poprzez podłączenie ich do zasilaczy awaryjnych UPS. Usługa monitoringu działania Geoportalu połączona jest z systemem powiadomienia e-mail oraz sms. Na wypadek awarii Administrator Systemu Informatycznego powiadamiany jest w/w sposób i jest w stanie określić poziom awarii usługi oraz systemu operacyjnego. W Starostwie funkcjonuje system elektronicznej kontroli dostępu do pomieszczeń, co umożliwia pełna kontrolę oraz rejestracje zdarzeń dotyczących osób mających dostęp do pomieszczeń. System kontroli dostępu działa w oparciu o dwie metody uwierzytelniania, za pomocą karty zbliżeniowej oraz za pomocą czytnika linii papilarnych. W celu ochrony najważniejszych lokalizacji zabezpieczenia wejścia dodatkowo jest chronione przez portierów/ochroniarzy. Wejścia osób trzecich do stref chronionych mogą się odbywać tylko w towarzystwie pracownika Starostwa.

W serwerowni zamontowane są detektory dymu oraz instalacja przeciwpożarowa z systemem gaszenia gazem. Zamontowana jest również instalacja alarmowa.W serwerowni oraz w pomieszczeniu gdzie znajduje się Centralny UPS zamontowane są czujniki temperatury, które są podłączone do systemu ZABBIX. W przypadku przekroczenia temperatury system ZABBIX wysyła powiadomienia do pracowników Zespołu ds. informatyzacji poprzez wiadomość SMS oraz wiadomości meilowe.

**2.3.3. Kopie zapasowe**

W Starostwie Powiatowym w Kielcach kopie bezpieczeństwa wykonywane są za pomocą Microsoft System Center Data Protection Manager, które wykonuje się dla każdego serwera jako pełna kopie systemu operacyjnego wraz z danymi właściwymi dla danego serwera, które podlegają codziennej aktualizacji i przechowywane są na dedykowanym serwerze. Kopie danych aktualizowane sporadycznie, przechowywane są na serwerach plikowych NAS. Kopie bezpieczeństwa wykonywane są z zachowaniem następujących cykli:

- w cyklu codziennym- w godzinach nocnych wykonywana jest przyrostowa kopia bezpieczeństwa;

- w cyklu tygodniowym- w sobotę wykonywana jest pełna kopia bezpieczeństwa;

- w cyklu miesięcznym – w ostatni piątek każdego miesiąca wykonywana jest pełna kopia bezpieczeństwa miesięczna.

**2.4. powiat pińczowski**

**2.4.1**. **Analiza lokalizacji pomieszczenia serwerowni.**

Siedziba Wydziału Geodezji, Kartografii , Katastru i Gospodarki Nieruchomościami Starostwa Powiatowego w Pińczowie mieści się (poza głównym obiektem urzędu ) przy ulicy Złota 7 w Pińczowie. Wydział zajmuje pomieszczenia I pietra (ok. 210 m2 powierzchni). Na potrzeby Wydziału urządzona zostałaserwerownia, wyposażona w serwery: 5xblade ( e-świętokrzyskie), 1 x kontroler domeny wydziału, 1x geoportal powiatowy, wydzielone linie zasilania, z osobnym zabezpieczeniem, potrzymanie UPS 2x 3000 VA, 2 x 1000 VA, internet, w tym łącze i dostawca (dywersyfikacja) - orange DSL 40/4 Mbit, łącze radiowe jako zapas.

**2.4.2.** **Zabezpieczenia**

Pomieszczenie serwerowni wyposażone jest w instalację p.poż., klimatyzację oraz zabezpieczone systemem alarmowym działającym nacałym wydziale. Wejście do pomieszczenia zabezpieczone jest przed niepowołanym dostępem - dostęp za pomocą karty lub kodu. Ponadto realizowany jest monitoring warunków klimatycznych i zadań stałych (np. poprawność wykonania kopii) oraz automatyzacja procesu inicjacji systemów po awarii - bez udziału pracownika - systemy uruchamiają się automatycznie.

**2.4.3. Kopie bezpieczeństwa**

Kopia bezpieczeństwa wykonywana jest automatycznie codziennie na dysk zlokalizowany w serwerowni oraz w tygodniu na dysk ulokowany w drugim budynku Starostwa Powiatowego w Pińczowie.

1. **Analiza istniejących zagrożeń, działania na wypadek awarii.**

**3.1. Analiza istniejących zagrożeń w Powiecie Buskim, Jędrzejowski, Kieleckim i Pińczowskim.**

We wszystkich Starostwach Powiatowych realizujących wspólnie Projekt e-GEODEZJA , występują typowe dla pomieszczeń infrastruktury informatycznej incydenty. Zaliczamy do nich:

* 1. awaria łącza internetowego;
  2. awaria klimatyzacji;
  3. awaria serwera;
  4. awaria urządzeń aktywnych sieci komputerowej;
  5. awaria infrastruktury sieciowej;
  6. awaria oprogramowania.

Za awarię rozumie się stan niesprawności w/w elementów systemu uniemożliwiające jego funkcjonowanie, występujący nagle i powodujący jego niewłaściwe działanie lub całkowite unieruchomienie.

Przyczynami wyżej wymienionych incydentów mogą być:

1. zdarzenie losowe ( awaria zasilania, zalanie pomieszczenia serwerowni, pożar, awaria systemu klimatyzacji);
2. ingerencja osób z zewnątrz (np.atak hakerski);
3. umyślne lub nieumyślne działanie osób zatrudnionych w Starostwach powiatów: buskiego, jędrzejowskiego, kieleckiego i pińczowskiego.
   1. **Działania na wypadek awarii**

W sytuacji wystąpienia awarii systemu informatycznego , Starostwa podejmują czynności zapewniające przywrócenie do pierwotnej zdolnościdziałania systemu.

**3.2.1. powiat Buski**

W Starostwie Powiatowym w Busko-Zdroju za realizację procedury przywrócenia zdolności działania systemu odpowiadają:

- Kierownik jednostki;

- Inspektor Ochrony Danych Osobowych;

- Administrator Systemu Informatycznego.

**3.2.1.1 Działania zapewniające przywrócenie zdolności realizacji działania Geoportalu**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Funkcja** | **Opis działań** | **Potrzebne zasoby** |
| 1. | Zweryfikować zasadność zgłoszenia od użytkownika | Sprawdzić, czy zgłoszenie dotyczy incydentu spowodowanego awarią systemu. | Zapewnić dostęp do infrastruktury informatycznej |
| 2. | Ustalić źródło awarii | Ustalić co jest przyczyną awarii:  - brak połączenia z siecią Internet  - przerwa w zasilaniu prądem  - wadliwe działanie sprzętu  - wadliwe działanie klimatyzacji  - wadliwe działanie aplikacji Geoportalu  - wadliwe działanie systemu operacyjnego, na którym zainstalowano Geoportal | Zapewnić:  - dostęp do serwerowni oraz do urządzeń i serwerów, które mogły ulec awarii  - kontakt z osobą, która w porze poza godzinach pracy urzędu może pobrać klucze w celu otwarcia budynku i udostępnienia pomieszczeń  - w przypadku awarii zamków wezwać ślusarza  - w przypadku awarii zasilania elektrycznego wezwać uprawnionego elektryka  - w przypadku awarii klimatyzacji wezwać firmę do usunięcia usterki |
| 3. | Określić skalę awarii | Ustalić czy awaria powoduje zatrzymanie pracy Geoportalu | Zapewnić kontakt z kluczowymi pracownikami odpowiedzialnymi za system informatyczny. |
| 4. | Ustalić czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji | Działanie to ma na celu zweryfikowanie, czy odnowienie usługi Geoportalu będzie w dotychczasowej lokalizacji, czy w lokalizacji alternatywnej. | Zapewnić:  - możliwość uruchomienia usługi w lokalizacji alternatywnej  - infrastrukturę sieciową  - zasilanie prądem |
| 5. | Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić usługę | W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu usług na stałe na inny serwer). | Zapewnić:  - w uzgodnieniu w przełożonymi, środków na zakup elementów niezbędnych do ponownego uruchomienia systemu oraz usług |
| 6. | Zweryfikować możliwość przeniesienia usług na inny serwer | Sprawdzić, czy usługa może być uruchomiona na dowolnym działającym poprawnie serwerze. | - |
| 7. | Przygotować serwer zastępczy | Jako serwer można wykorzystać dowolny komputer, który należy odpowiednio skonfigurować. Po uruchomieniu usług na serwerze zastępczym należy przetestować ich działanie. | Zapewnić:  - sprzęt dowolnego typu, który umożliwi uruchomienie usług w podstawowym ich zakresie. |
| 8. | Przywrócić funkcjonowanie usługi Geoportalu / systemu | Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć maszynę i usługi z kopii zapasowych | Zapewnić:  - dostęp do najbardziej aktualnej wersji portalu  - dostęp do aktualnej bazy danych. |
| 9. | Sprawdzenie aplikacji / systemu | Po migracji i uruchomieniu należy zweryfikować prawidłowe funkcjonowanie usług zainstalowanych na serwerze. | - |
| 10. | Uruchomienie usługi w trybie produkcyjnym | Po uruchomieniu usług należy powiadomić przełożonego o postępie. | Zapewnić:  - kontakt z kluczowymi pracownikami i kierownikami |

**3.2.2 powiat Jędrzejowski**

W Starostwie Powiatowym w Jędrzejowie za realizację procedury przywrócenia zdolności wadliwego elementu odpowiadają:

- Kierownik jednostki;

- Administrator Systemu Informatycznego;

- Inspektor Ochrony Danych Osobowych (Audytor).

**3.2.2.1. Działania zapewniające przywrócenie zdolności realizacji działania Geoportalu**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Funkcja** | **Opis działań** | **Potrzebne zasoby** |
| 1. | Zweryfikować zasadność zgłoszenia od użytkownika | Sprawdzić, czy zgłoszenie dotyczy incydentu spowodowanego awarią systemu. | Zapewnić dostęp do infrastruktury informatycznej |
| 2. | Ustalić źródło awarii | Ustalić co jest przyczyną awarii:  - brak połączenia z siecią Internet  - przerwa w zasilaniu prądem  - wadliwe działanie sprzętu  - wadliwe działanie klimatyzacji  - wadliwe działanie aplikacji Geoportalu  - wadliwe działanie systemu operacyjnego, na którym zainstalowano Geoportal | Zapewnić:  - dostęp do serwerowni oraz do urządzeń i serwerów, które mogły ulec awarii  - kontakt z osobą, która w porze poza godzinach pracy urzędu może pobrać klucze w celu otwarcia budynku i udostępnienia pomieszczeń  - w przypadku awarii zamków wezwać ślusarza  - w przypadku awarii zasilania elektrycznego wezwać uprawnionego elektryka  - w przypadku awarii klimatyzacji wezwać firmę do usunięcia usterki |
| 3. | Określić skalę awarii | Ustalić czy awaria powoduje zatrzymanie pracy Geoportalu | Zapewnić kontakt z kluczowymi pracownikami odpowiedzialnymi za system informatyczny. |
| 4. | Ustalić czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji | Działanie to ma na celu zweryfikowanie, czy odnowienie usługi Geoportalu będzie w dotychczasowej lokalizacji, czy w lokalizacji alternatywnej. | Zapewnić:  - możliwość uruchomienia usługi w lokalizacji alternatywnej  - infrastrukturę sieciową  - zasilanie prądem |
| 5. | Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić usługę | W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu usług na stałe na inny serwer). | Zapewnić:  - w uzgodnieniu w przełożonymi, środki na zakup elementów niezbędnych do ponownego uruchomienia systemu oraz usług |
| 6. | Zweryfikować możliwość przeniesienia usług na inny serwer | Sprawdzić, czy usługa może być uruchomiona na dowolnym działającym poprawnie serwerze. | - |
| 7. | Przygotować serwer zastępczy | Jako serwer można wykorzystać dowolny komputer, który należy odpowiednio skonfigurować. Po uruchomieniu usług na serwerze zastępczym należy przetestować ich działanie. | Zapewnić:  - sprzęt dowolnego typu, który umożliwi uruchomienie usług w podstawowym ich zakresie. |
| 8. | Przywrócić funkcjonowanie usługi Geoportalu / systemu | Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć maszynę i usługi z kopii zapasowych | Zapewnić:  - dostęp do najbardziej aktualnej wersji portalu  - dostęp do aktualnej bazy danych. |
| 9. | Sprawdzenie aplikacji / systemu | Po migracji i uruchomieniu należy zweryfikować prawidłowe funkcjonowanie usług zainstalowanych na serwerze. | - |
| 10. | Uruchomienie usługi w trybie produkcyjnym | Po uruchomieniu usług należy powiadomić przełożonego o postępie. | Zapewnić:  - kontakt z kluczowymi pracownikami i kierownikami |

**3.2.3. powiat Kielecki**

**3.2.3.1. Działania zapewniające przywrócenie zdolności realizacji działania Geoportalu**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Funkcja** | **Opis działań** | **Potrzebne zasoby** |
| 1. | Zweryfikować zasadność zgłoszenia od użytkownika | Sprawdzić, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego. | Zapewnić dostęp do infrastruktury informatycznej na stanowisku skąd pochodzi zgłoszenie.  Odpowiedzialny: Kierownik Zespołu ds. Informatyzacji, Pełnomocnik ds. SZBI, ASI, ADO. |
| 2. | Ustalić źródło awarii | Ustalić, co jest przyczyną awarii:  - przerwa w zasilaniu prądem,  - brak połączenia z siecią Internet,  - wadliwe działanie sprzętu,  - wadliwe działanie aplikacji,  - wadliwe działanie systemu, na którym uruchomiona jest aplikacja. | Zapewnić:  - dostęp do serwerowni oraz do urządzeń i serwerów, które mogły ulec awarii,  - kontakt z osobą, od której można pobrać klucze do serwerowni, w przypadku , gdy nie działa system kontroli dostępu,  - w przypadku blokady zamka wezwać konserwatora,  - w przypadku awarii zasilania elektrycznego sprawdzić czy działa zasilanie awaryjne ( Centralny UPS, agregat prądotwórczy). Powiadomić Referat Infrastruktury o awarii zasilania.  Odpowiedzialny: Kierownik Zespołu ds. Informatyzacji, Pełnomocnik ds. SZBI, ASI, ADO. |
| 3. | Określić skalę awarii | Ustalić czy awaria powoduje zatrzymanie pracy:  - jednego stanowiska pracy lub wydziału,  -kilku wydziałów,  Całego urzędu wraz z usługą Geoportalu | Zapewnić:  - kontakt z kluczowymi pracownikami wydziałów.  Odpowiedzialny: Kierownik Zespołu ds. Informatyzacji, Pełnomocnik ds. SZBI, ASI, ADO. |
| 4. | Ustalić czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji | Działanie to ma na celu zweryfikowanie, czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacji alternatywnej. | Zapewnić:  - możliwość uruchomienia potrzebnych usługi w lokalizacji  - infrastrukturę sieciową, zasilanie prądem.  Odpowiedzialny: Kierownik Zespołu ds. Informatyzacji, Pełnomocnik ds. SZBI, ASI, ADO. |
| 5. | Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić aplikację. | W przypadku braku możliwości zakupu, należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na stałe na inny serwer). | Zapewnić:  - środki na zakup elementów niezbędnych do ponownego uruchomienia systemu.  Odpowiedzialny: Kierownik Zespołu ds. Informatyzacji, Pełnomocnik ds. SZBI, ASI, ADO. |
| 6. | Zweryfikować możliwość przeniesienia aplikacji na inny serwer. | Sprawdzić, czy aplikacja może być uruchomiona na którymś z działających poprawnie serwerów. | Odpowiedzialny: ASI |
| 7. | Przygotować serwer zastępczy. | Po uruchomienie aplikacji na serwerze zastępczym należy przetestować jej działanie. | Zapewnić:  - maszynę dowolnego typu, która w podstawowym zakresie pozwoli na uruchomienie podstawowych usług.  Odpowiedzialny: ASI |
| 8. | Podjąć decyzję o terminie odtworzenia maszyny. | W razie konieczności należy skontaktować się z właściwymi kierownikami komórek organizacyjnych. | Odpowiedzialny: ASI, Kierownik ds. Informatyzacji. |
| 9. | Przywrócić funkcjonowanie aplikacji/ systemu | Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć aplikację z kopii zapasowych. | Zapewnić:  - dostęp do najbardziej aktualnej wersji aplikacji,  - dostęp do aktualnej bazy danych.  Odpowiedzialny: ASI |
| 10. | Sprawdzenie aplikacji / systemu | Po przeniesieniu/uruchomieniu należy zweryfikować prawidłowe funkcjonowanie aplikacji/systemów zainstalowanych na serwerze. | Zapewnić:  - kontakt z kluczowymi pracownikami wydziału mogącymi przetestować prawidłowość funkcjonowania systemów i aplikacji.  Odpowiedzialny: ASI |

**3.2.4. powiat Pińczowski**

W ramach prowadzonej w Starostwie Powiatowym w Pińczowie - Polityki Bezpieczeństwa Danych Osobowych, *Zarządzeniem Starosty Pińczowskiego nr 20.2018 z dnia 07.06.2018 roku*, ustanowiono Administratora Systemu Informatycznego powierzając mu miedzy innymi następujące obowiązki :

1. zapewnienia optymalnej ciągłości działania systemu informatycznego,
2. nadzór nad pracami firm zewnętrznych przeprowadzających prace przy naprawach, konserwacji systemów informatycznych, naprawcze,
3. właściwą konfigurację systemu informacyjnego , zapewniającą jego bezpieczeństwo i ograniczenie dostępu do danych przez osoby nieupoważnione,
4. nadzór nad sporządzaniem kopii bezpieczeństwa , instalację i konfigurację na poszczególnych stacjach roboczych,
5. okresowe weryfikacje zainstalowanego oprogramowania.