Dokumentacja środowiska e-podręczniki

Spis treści:

1. Klaster aplikacyjny

Portal realizuje warstwę prezentacji treści i jest głównym składnikiem platformy epodręczniki. Odpowiada za graficzną prezentację modeli danych, treści w formatach źródłowych, a także zapewnia warstwę nawigacji na poziomie strony web. Na prezentację treści składa się kilka obszarów, do których użytkownik ma dostęp za pomocą odpowiednich widoków. Głównymi elementami są CMS, który jest systemem zarządzania treścią i pozwala na przygotowanie strony startowej platformy epodręczniki oraz na dodawanie materiałów informacyjno-promocyjnych, biblioteka, która odpowiada za prezentację listy podręczników, biorąc pod uwagę podział podręczników ze względu na poziomy nauczania i klasy, oraz czytnik, który odpowiada za prezentację treści podręczników.

Lista instancji:

- app1 - 10.90.54.201
- app2 - 10.90.54.202
- app3 - 10.90.54.203
- app4 - 10.90.54.204
- app-celery - 10.90.54.209

Działające usługi:

epo-celery - odpowiada za akcje portalu wykonywane w tle i komunikację z innymi częściami systemu, działa na instancji app-celery
epo-listener - odpowiada za akcje portalu wykonywane w tle, działa na instancji app-celery uruchamaina na userze „epo”
epo-portal - aplikacja django odpowiedzialna za serwowanie aplikacji epodreczniki działa na nodach „appX”, jest uruchamiana na użytkowniku „epo”
nginx – serwer www, działa na nodach „appX”

PortalDB
Baza danych PostgreSQL używana przez portal.

Lista instancji:

- portal-db1 - 10.90.54.221

Działające usługi:

- **postgresql** - serwer bazodanowy posiadający dane portalu
- **redis-server**- redis, baza cache'u dla całego portalu

2. Klaster GlusterFS

Klaster GlusterFS, odpowiada za przechowywanie plików statycznych.

Lista instancji:

- storage1 - 10.90.54.211
- storage2 - 10.90.54.212

3. Kontekst użytkownika

Kontekst użytkownika jest komponentem realizującym zagadnienie personalizacji treści oraz środowiska pracy na platformie. Dotyczy on zarówno samych treści, jak i sposobu nawigacji po portalu. Klaster bazodanowy cassandry, przechowuje informacje o aktualnie wykonywanych zadaniach dla danego użytkownika.

Lista instancji:

- ku1 - 10.90.54.151
- ku2 - 10.90.54.152

4. Serwer kodujący treści

Serwer Kodujący (SK) jest odpowiedzialny za reagowanie na komunikaty z repozytoriów treści o utworzonych i zmodyfikowanych kolekcjach poprzez wygenerowanie ich formatów emisyjnych, a także na reagowanie na zmodyfikowane WOMI poprzez wygenerowanie zaktualizowanych formatów emisyjnych kolekcji, które z tych WOMI korzystają. Realizowaną przez SK funkcjonalnością jest generowanie formatów emisyjnych kolekcji - HTML, PDF, format dla aplikacji natywnych - w reakcji na zdarzenia modyfikacji kolekcji lub jej obiektów zależnych (WOMI, treści modułów). Wygenerowane formaty emisyjne są udostępniane za pomocą HTTP dla innych komponentów.

Lista instancji:

- skt1 - 10.90.54.51

Działające usługi:

- **epo-sk -** javowa aplikacja odpowiedzialna za przetwarzanie podręczników

5. Otwarte repozytorium treści

Otwarte Repozytorium Treści to system, w którym przechowywane i udostępniane są treści oraz metadane obiektów składowych e-podręczników, przyjmowane nowe i zmodyfikowane obiekty od użytkowników. ORT informuje pozostałe komponenty o zmianach w treści i w metadanych obiektów, konwertuje źródłowe obrazy WOMI do formatów emisyjnych, przetwarza wybrane WOMI do formatów emisyjnych oraz umożliwia wyszukiwanie obiektów na podstawie metadanych.

Lista instancji:

- ort1 - 10.90.54.31

Działające usługi:

- **epo-dlibra** - javowa aplikacja dLibry
- **epo-tomcat** – manager aplikacji webowych (zarządza usługą dlibry)

6. Serwer wymiany komunikatów

Usługa służy do wymiany komunikatów pomiędzy poszczególnymi komponentami o zdarzeniach zachodzących na platformie. Przekazywane wiadomości dotyczą przede wszystkim zdarzeń wprowadzenia zmian w plikach źródłowych lub w formatach emisyjnych podręczników, WOMI czy zasobów KZD.

Lista instancji:

- **skwpk1** - 10.90.54.91

Działające usługi:

- **rabbitmsq-server** – usługa kolejkowania zadań na platformie epodreczniki

7. System zarządzania katalogiem zasobów dodatkowych

System zarządzania Katalogu Zasobu Dodatkowych (KZD) umożliwia uprawnionym użytkownikom dodawanie nowych zasobów na podstawie plików umieszczonych na serwerze Ministerstwa Edukacji Narodowej (MEN), edycję wybranych metadanych zasobów za pomocą interfejstu użytkownika w portalu oraz usuwanie zasobów za pomocą interfejsu użytkownika w portalu.

Lista instancji:

- **szkzd1** - 10.90.54.71

8. Usługa wyszukiwania treści

Systemy odpowiadają za wyszukiwanie elementów w kontekście Katalogu Zasobów Dodatkowych (wyszukiwanie obiektów) oraz Biblioteki e-podręczników (wyszukiwanie pełnotekstowe). Wyszukiwanie obiektów na potrzeby Katalogu Zasobów Dodatkowych wykorzystuje silnik indeksu pełnotekstowego Elastic (Elasticsearch) natomiast wyszukiwanie pełnotekstowe wykorzystuje instancję silnika indeksu pełnotekstowego SOLR, który przechowuje w zdefiniowanym schemacie dane na potrzeby realizacji kwerend wyszukiwawczych.

Lista instancji:

- **uwt1_elastic** - 10.90.54.111
- **uwt2_solr** - 10.90.54.112

9. Otwarte Repozytorium Audio/Video

Systemy służące do przechowywania, przetwarzania oraz udostępniania treści audiowizualnych. Usługi dostępowe umożliwiają dodanie, aktualizację, usunięcie, sprawdzenie stanu materiału oraz pobranie formatu danego materiału (treści audio i/lub video). Repozytorium zapewnia przechowywanie materiałów. Na węzłach repozytorium działają trzy typy podsystemów, *manager*, który m.in. nadzoruje pracę repozytorium oraz proces tworzenia formatów, *snode*, który przechowuje i udostępnia formaty materiałów oraz *recoder*, który realizuje operacje rekodowania formatów materiałów.

Centralną bazą danych jest RepDB, która zawiera metadane wszystkich materiałów i formatów oraz informację o ich lokalizacji. Dodatkową bazą danych na węzłach typu snode i recoder jest MaterialFormatDB, w której przechowywane są metadane o formatach wraz z ich fizyczną lokalizacją w systemie plików.

Lista instancji:

- **orav1** - 10.90.54.11
- **orav2** - 10.90.54.12
- **orav3** - 10.90.54.13
- **orav4** - 10.90.54.14
- **orav5** - 10.90.54.15
- **orav6** - 10.90.54.16

Działające usługi:

- MSSQL Server
- Proca (usługa hostowania podsystemów)

10. Router, VPN i firewall

Load balancer, firewall, VPN oraz router środowiska.

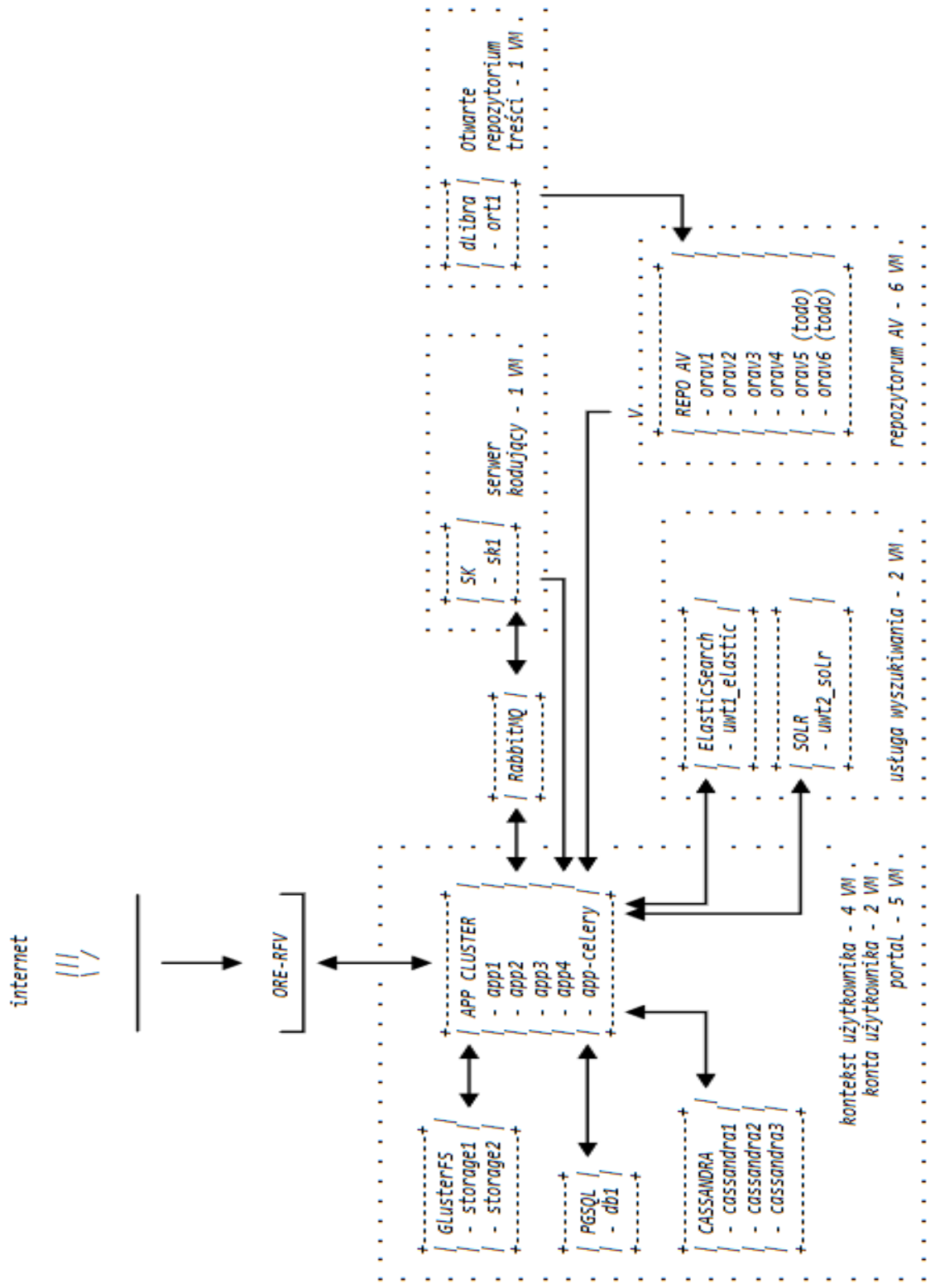
Lista instancji:

- **ORE-RFV –** adres publiczny 91.224.214.98, adres prywatny 10.90.54.254

Działające usługi:

- **OpenVPN** - odpowiada za zestawianie tunelu vpn do środowiska
- **HaProxy** - odpowiada za równoważenie obciążenia dla systemów pracujących w klastrze
- **Snort -** sieciowy system wykrywania włamań

11. Rysunek komunikacji wewnątrz środowiska



Instrukcja blokowania ataków typu DoS oraz DDoS

1. CEL

Celem niniejszej instrukcji jest opisanie procedury działań podejmowanych w celu zablokowania lub zminimalizowania skutków ataku DDoS na środowisko systemu informatycznego ORE.

2. ZAKRES

Instrukcja dla osób odpowiedzialnych za administrowanie systemów informatycznych.

3. DEFINICJE

Administrator systemu informatycznego - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego.

System informatyczny - zespół współpracujących ze sobą urządzeń, systemów operacyjnych, oprogramowania biznesowego oraz narzędziowego, które stosowane są w systemie hostingowym ORE.

Atak DoS/DDoS- atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów (Denial of Service), może być przeprowadzany równocześnie z wielu komputerów (Distributed Denial of Service)

4. Obrona przed atakiem DoS

W przypadku wykrycia ataku DoS pochodzącego z jednego konkretnego źródła (adresu IP), adres atakującego zostanie zablokowany na routerze dostawcy, aby nie wpływać na zajętość pasma udostępnianego środowisku hostingowemu.

Ponadto w zależności od atakowanej usługi zostaną podjęte próby jej rekonfiguracji w celu obsługi zwiększonego ruchu, np. poprzez tymczasowe zwiększenie dostępnych zasobów, lub zmianę konfiguracji usługi.

5. Ograniczenie skutków ataku DDoS

W przypadku wykrycia ataku DDoS zostaną podjęte próby zablokowania na routerze dostawcy łącza, najbardziej aktywnych adresów lub zakresów adresów IP.

W przypadku rozległych ataków DDoS niemożliwych do zablokowania i pochodzących z różnych zagranicznych adresów IP, rozgłaszanie zaatakowanej docelowej klasy IP środowiska zostanie wyłączone na łączach zagranicznych i środowisko stanie się dostępne tylko dla polskich Internautów.

W przypadku przedłużającego się ataku trwającego ponad kilka minut, lub ataku o wolumenie przekraczającym przepustowość łącz dostawcy, zostaną zgłoszone mailowo lub telefonicznie prośby do zespołów operacyjnych dostawców łącz, w celu próby zablokowania ruchu na ich routerach brzegowych.

Instrukcja blokowania nieautoryzowanego dostępu

1. CEL

Celem niniejszej instrukcji jest opisanie procedury działań podejmowanych w celu zablokowania nieautoryzowanego dostępu do środowiska systemu informatycznego.

2. ZAKRES

Instrukcja dla osób odpowiedzialnych za administrowanie systemów informatycznych.

3. DEFINICJE

Administrator systemu informatycznego - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego.

System informatyczny - zespół współpracujących ze sobą urządzeń, systemów operacyjnych, oprogramowania biznesowego oraz narzędziowego, które stosowane są w systemie hostingowym ORE.

Dostęp nieautoryzowany - działanie naruszające istniejącą politykę bezpieczeństwa

4. BLOKADA DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

W celu zablokowania nieautoryzowanego dostępu należy jak najszybciej na podstawie dostępnych logów zidentyfikować adres IP oraz sposób w jaki dostęp został uzyskany.

W pierwszej kolejności nastąpi zablokowanie na routerze oraz w razie potrzeby na firewallu adresu IP z którego nastąpił nieautoryzowany dostęp.

Kolejnym krokiem jest wyłączenie usługi podatnej na nieautoryzowany dostęp do czasu zidentyfikowania i naprawienia przyczyny, oraz dogłębna analiza dostępnych logów w celu zidentyfikowania przyczyny i skutków incydentu.

Instrukcja obsługi żądania dostępu

1. CEL

Celem niniejszej instrukcji jest opisanie zasad nadawania uprawnień użytkownikom oraz zasad dotyczących korzystania z systemów informatycznych działających.

2. ZAKRES

Instrukcja dla osób odpowiedzialnych za administrowanie systemów informatycznych.

3. DEFINICJE

Administrator systemu informatycznego - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego.

System informatyczny - zespół współpracujących ze sobą urządzeń, systemów operacyjnych, oprogramowania biznesowego oraz narzędziowego, które stosowane są w systemie hostingowym ORE.

Maximo – Oprogramowanie IBM SmartCloud Control Desk, kompleksowe rozwiązanie do zarządzania zasobami i usługami informatycznymi, które posiada zautomatyzowaną obsłudze zgłoszeń serwisowych, zarządzaniu zmianami oraz optymalizacji zarządzania cyklem życia zasobów informatycznych.

4. WNIOSKOWANIE O NADANIE DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

Wniosek o nadanie uprawnień do systemu informatycznego lub jego części polega na zarejestrowaniu zgłoszenia w systemie Maximo. Wniosek powinien zawierać informacje o osobie dla której zostaną przydzielone uprawnienia oraz okres ich ważności. Należy podać także cel ich nadania oraz poziom uprawnień jakie mają być nadane zarówno do dostępu zdalnego jak i poszczególnych systemów, aplikacji, usług. Przed nadaniem uprawnień należy potwierdzić informacje mailowo. Mail należy załączyć w zgłoszeniu.

Instrukcja powiadamiania o incydencie

1. CEL

Celem procedury jest zapewnienie odpowiedniego postępowania na wypadek wystąpienia zdarzenia lub incydentu związanego z Bezpieczeństwem Informacji.

2. ZAKRES STOSOWANIA

a. Zakres podmiotowy

Instrukcja obowiązuje wszystkich pracowników.

b. Zakres przedmiotowy

Instrukcja obowiązuje w przypadku wystąpienia incydentu lub zdarzenia związanego z bezpieczeństwem informacji, które mogą mieć miejsce w każdym z realizowanych przez firmę procesów lub działań.

3. DEFINICJE

System informatyczny - zespół współpracujących ze sobą urządzeń, systemów operacyjnych, oprogramowania biznesowego oraz narzędziowego, które stosowane są w systemie hostingowym ORE.

Zdarzenie - zdarzenie związane z bezpieczeństwem informacji jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem. Zdarzenie to potencjalny incydent.

Incydent – incydent związany z bezpieczeństwem informacji jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji

4. OPIS POSTĘPOWANIA

a. Identyfikacja zdarzenia /incydentu

Źródłem informacji dotyczących zdarzenia /incydentu mogą być między innymi:

- Informacje wynikające z wykonywanych procedur monitoringu, stanu skuteczności systemów zabezpieczeń, spostrzeżeń.
- Spostrzeżeń pracowników, osób pracujących nad utrzymaniem systemu informatycznego, zgłoszeń stron zainteresowanych w tym klienta. Wyników działań nadzorczo-kontrolnych w poszczególnych obszarach
- Wyniki przeglądów i audytów w ramach których zidentyfikowane zostanie zdarzenie lub incydent

b. Reakcja na zdarzenie /incydent

Każdy pracownik firmy oraz osoba pracująca na rzecz utrzymania systemu informatycznego, którzy zidentyfikują zdarzenie /incydent zobowiązani są do tego, aby, jeśli tylko leży to w zakresie ich kompetencji, uruchomić odpowiednie działania mające na celu zminimalizowanie prawdopodobieństwa wystąpienia danego zdarzenia /incydentu a w przypadku ich materializacji do uruchomienia działań mających na celu minimalizowanie potencjalnych lub rzeczywistych skutków.

Odpowiedź na zdarzenie /incydent powinna być adekwatna do potencjalnych skutków jakie dane zdarzenie /incydent może wywołać lub wywołuje.

c. Zgłoszenie zdarzenia /incydentu

Zgłoszenie zdarzenia /incydentu następuje poprzez system Maximo.

Instrukcja zabezpieczenia danych z incydentu bezpieczeństwa

1. CEL

Celem procedury jest zapewnienie odpowiedniego postępowania z danymi wystąpienia zdarzenia lub incydentu związanego z Bezpieczeństwem Informacji.

2. ZAKRES STOSOWANIA

- Zakres podmiotowy

Instrukcja obowiązuje wszystkich pracowników.

- Zakres przedmiotowy

Instrukcja obowiązuje w przypadku wystąpienia incydentu lub zdarzenia związanego z bezpieczeństwem informacji, które mogą mieć miejsce w każdym z realizowanych przez firmę procesów lub działań.

3. DEFINICJE

System informatyczny - zespół współpracujących ze sobą urządzeń, systemów operacyjnych, oprogramowania biznesowego oraz narzędziowego, które stosowane są w systemie hostingowym ORE.

Zdarzenie - zdarzenie związane z bezpieczeństwem informacji jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas

sytuację, która może być związana z bezpieczeństwem. Zdarzenie to potencjalny incydent.

Incydent – incydent związany z bezpieczeństwem informacji jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji

4. OPIS POSTĘPOWANIA

Zgłoszenie zdarzenia /incydentu następuje poprzez udokumentowanie faktu ich wystąpienia w systemie informatycznym Maximo. Wszystkie informacje dotyczące incydentu w postaci logów systemowych, logów aplikacyjnych, migawki nagrań wideo itd., należy dołączyć do zgłoszenia w systemie Maximo. W zgłoszeniu należy również dokładnie opisać zaistniałą sytuację wraz w datą i czasem jego zaistnienia, wykrycia.

ZARZĄDZANIE ZDARZENIEM (IMP) ORAZ PLAN CIĄGŁOŚCI DZIAŁANIA (BCP)

1 **ZDARZENIE: Awaria Infrastruktury Centrum Przetwarzania Danych**

2 CEL:
1. Zapewnienie ciągłości działania procesów
2. Minimalizacja strat oraz utraconych potencjalnych korzyści
3. Zapewnienie powrotu do działalności na normalnym poziomie w zaplanowanym czasie przy zidentyfikowanych na etapie planowania kosztach niniejszych działań i zasobów wykorzystanych do tego celu

3 ZAKRES: *Działanie personelu nadzorującego funkcjonowanie Centrum Przetwarzania Danych*

4 Odpowiedzialny za nadzorowanie *Planu*: *Dyrektor Działu Technicznego*

UWAGI odnośnie zdarzenia

Awaria infrastruktury serwerowej, sieciowej, pomocniczej (klimatyzacja, zasilanie, konstrukcja budynku) uniemożliwiająca kontynuowanie działania CPD.

Potencjalne straty w przypadku materializacji zdarzeń:

Utrata siedziby możne nastąpić na skutek:
1. *Pożaru*
2. *Powodzi i innej klęski żywiołowej*
3. *Inne nieprzewidziane okoliczności uniemożliwiające realizację procesów na normalnym poziomie w danej lokalizacji.*

Straty związane mogą być z:
- utratą wartości materialnej (środki trwałe: sprzęt teleinformatyczny)

- utrata potencjalnych korzyści wynikająca z braku możliwości realizacji działań
- uszkodzenia sprzętu zainstalowanego w CPD (zarówno sprzętu IT jak i infrastruktury: UPS, zasilanie, klimatyzacja)
- niezapewnienie ciągłości działania świadczonych usług na skutek zatrzymania działania systemów w CPD.

PRIORYTETY CIĄGŁOŚCI DZIAŁANIA

Priorytet krytyczny.

Uruchomienie obu procesów: handlowego i serwisowego ma ten sam priorytet

PLAN ZARZĄDZANIA ZDARZENIEM (IMP)

Identyfikacja zdarzenia

Odczyt informacji o niedostępności systemów oraz urządzeń wchodzących w skład infrastruktury CPD z systemu monitoringu.

W przypadku wystąpienia zagrożenia, które spowoduje brak możliwości korzystania ze stanowisk pracy znajdujących się w danej lokalizacji to samo zdarzenie może wiązać się z ryzykiem dla zdrowia i życia pracowników.

Każdy z pracowników może uruchomić plan zarządzania zdarzeniem. Powinien to zrobić niezwłocznie gdy tylko zdarzenie zostanie przez niego zidentyfikowane w celu zapewnienia jak najkrótszego czasu ekspozycji personelu i mienia na dane zagrożenie. Im krótszy czas ekspozycji na zagrożenie tym mniejsze potencjalne skutki.

W przypadku zdarzeń stanowiących zarazem zagrożenie dla życia i zdrowia ludzi obowiązują instrukcje i inne regulacje z zakresu BHP i p.poż..

Wszystkich obowiązuje kolejność ratowania życia i zdrowia przed ratowaniem mienia oraz zaalarmowania wszystkich potencjalnie zagrożonych. Działania mające na celu eliminację lub minimalizację skutków danego zagrożenia można prowadzić wyłącznie wtedy kiedy nie zagraża to życiu i zdrowiu.

Odpowiedzialny za zarządzanie zdarzeniem: **Dyrektor Działu Technicznego**

Postępowanie ze zdarzeniem

l.p.	***Działanie***	***Odpowiedzialny***
1	*Zaalarmowanie osób w przypadku zagrożenia ich zdrowia lub życia*	*Identyfikujący zdarzenie (każda osoba)*
2	*Próba powstrzymania zagrożenia we własnym zakresie – jeśli możliwe*	*Identyfikujący zdarzenie (każda osoba)*
3	*Zaalarmowanie odpowiednich służb ratownictwa* ***TELEFON ALARMOWY: 112 z TELEFONÓW KOMÓRKOWYCH***	*Identyfikujący zdarzenie (każda osoba)*
4	*W przypadku potrzeby ewakuacja pracowników i interesariuszy z miejsca zagrożenia - postępowanie zgodnie z zasadami ewakuacji* *W przypadku potrzeby udzielenie pierwszej pomocy rannym*	*Wyznaczona osoba odpowiedzialna za ewakuację z ramienia firmy lub właściciela obiektu* *Osoby z uprawnieniami do udzielania pierwszej pomocy*
5	*Zakres czynności:* *Zidentyfikować wszystkie zaobserwowane anomalie w trakcie zaistnienia awarii infrastruktury CPD.*	*Dyżurny Centrum Monitoringu*
6	*Poinformować osobę odpowiedzialną za zarządzanie zdarzeniem*	*Dyżurny Centrum Monitoringu*
7	*Raportowanie:* *Należy rejestrować czynności, zdarzenia zaistniałe w trakcie wystąpienia awarii. Jeżeli nie jest to możliwe w systemie Maximo, należy dokonać odręcznych zapisów.*	*Dyżurny Centrum Monitoringu*
8	*Raportowanie:* *Poinformowanie Zarządu Spółki Infomex o zaistniałej sytuacji.*	*Odpowiedzialny za zarządzanie zdarzeniem*
9	*Analiza problemu:* *Analiza zaistniałej sytuacji celem podjęcia odpowiednich kroków naprawczych*	*Odpowiedzialny za zarządzanie zdarzeniem Zarząd Spółki Infomex*
10	*Odtworzenie środowiska CPD w zastępczej lokalizacji.* *Podjęcie działań naprawczych, odtworzenie systemów z kopii zapasowych w nowym środowisku.*	*Odpowiedzialny za zarządzanie zdarzeniem*

UWAGI:

1.

Zasoby niezbędne do zarządzania zdarzeniem

Członek Zarządu Spółki Infomex
Dyrektor Działu Technicznego
Dyżurny Centrum Monitoringu

PLAN CIĄGŁOŚCI DZIAŁANIA (BCP)

Odpowiedzialny za inicjowanie Planu Ciągłości Działania

Dyrektor DT

Okoliczności inicjacji Planu Ciągłości Działania

Brak możliwości kontynuacji działania Centrum Przetwarzania Danych

Sposób inicjacji Planu Ciągłości Działania

Polecenie Dyrektora DT, przekazane bezpośrednio, telefonicznie lub za pośrednictwem e-mail. Polecenie przekazane zostaje do Centrum Monitoringu

Skład zespołu BCP

Nazwisko i imię	*stanowisko*	*Dane kontaktowe*	*Funkcja w zespole /odpowiedzialność*
	Członek Zarządu		*Decydent*
	Dyrektor DT		*Koordynator*
	Dyrektor Logistyki		*Odpowiedzialny za zakupy*
	Dyżurny Centrum Monitoringu		*Rejestracja zdarzeń, przekazywanie informacji o statusie rozwiązania problemu*

Komunikacja wewnętrzna oraz zewnętrzna

W ramach Planu Ciągłości Działania należy utrzymywać bieżącą komunikację w zakresie przebiegu działań oraz zarządzania nimi z niżej przedstawionymi jednostkami organizacyjnymi, Organizacjami zewnętrznymi oraz w przypadku potrzeby interesariuszami.

Jednostka /Organizacja /Interesariusz	*Komunikacja w zakresie*	*Linie i sposób łączności* */Podać dane kontaktowe/*	*Odpowiedzialny za komunikację*	*Termin /moment w którym musi nastąpić komunikacja*
Wewnętrznie	*Przekazanie Dyrektorowi, klientom informacji o awarii CPD*	*telefonicznie*	*Dyżurny Centrum Monitoringu*	*Natychmiast po pojawieniu się niekorzystnego trendu klimatycznego w CPD*
Wewnętrznie	*Przekazanie informacji o zaistniałej sytuacji do Zarządu*	*Ustnie lub telefonicznie*	*Dyrektor DT*	*W pierwszym możliwym terminie liczonym od otrzymania informacji od Dyżurnego CM*
Wewnętrznie	*Przygotowanie informacji o cenie, dostawcy oraz najbliższym możliwym terminie dostawy urządzeń*	*e-mail*	*Dyrektor Logistyki*	*W pierwszym dniu roboczym liczonym od momentu otrzymania informacji*

Wewnętrznie	*Podjęcie decyzji o dokonaniu zakupu najmu koniecznych zasobów.*	*Pisemnie*	*Zarząd*	*Bezpośrednio po otrzymaniu informacji o niemożliwości naprawy uszkodzonych jednostek*
Wewnętrznie	*Poinformowanie Dyrektora Działu Technicznego o terminie dostawy zamówionych jednostek*	*Ustnie lub telefonicznie lub via e-mail*	*Dyrektor Logistyki*	*Niezwłocznie po uzyskaniu od dostawcy potwierdzonej informacji*
Podmiot zewnętrzny	*Uzgodnienie terminu instalacji nowych urządzeń i odzyskaniu sprawności CPD*	*e-mail*	*Dyrektor DT*	*Niezwłocznie po otrzymaniu informacji od Dyrektora Logistyki*

Zasoby niezbędne do realizacji Planu Ciągłości Działania

l.p	*Rodzaj zasobu*	*ilość*	*szacunkowa wartość*	*Źródło pozyskania*	*uwagi*
1	*Szafa rak*	*2*		*Zakup – Podmiot zewnętrzny*	*Ilość zależna od wyeliminowanych z działania jednostek*
2	*Klatka Blade plus 10 serwerów HP BL480*	*1*		*Zakup – Podmiot zewnętrzny*	*j/w*
3	*Macierz dyskowa*	*1*			

UWAGA

Działania które należy podjąć i zadania jakie należy wykonać
Wraz z odpowiedzialnymi i terminami ich realizacji
(czas wznowienia działania oraz poziom działania po wznowieniu- CELE wraz z priorytetami)

l.p.	*działanie*	*odpowiedzialny*	*Termin realizacji*
1	*Dokonanie zakupu określonej liczby i dostawa nowych urządzeń*	*Dyrektor Logistyki*	*Niezwłocznie po otrzymaniu informacji od Dyrektora DT*
2	*Instalacja nowych urządzeń i odtworzenia oprogramowania, test poprawności działania.*	*Dyrektor DT*	*Najszybszy możliwy termin bezpośrednio po dostawie jednostek.*
3	*Podniesienie systemów, przekazanie informacji o uruchomieniu systemów*	*Dyrektor DT*	*Najszybszy możliwy termin bezpośrednio po dostawie jednostek.*

Całkowity czas trwania uruchomienia działalności na minimalnym poziomie – działania priorytetowe (RTO): *2 dni……*

Całkowity czas trwania powrotu do normalnej działalności (standardowe koszty działalności) (MTPoD): *7 dni……..*

Proces wycofania planu w przypadku ustąpienia zdarzenia

1. *Przekazanie informacji przez Dyrektora DT do Dyrektora Logistyki o rezygnacji z zakupów*
2. *Przekazanie informacji przez Dyrektora DT do Inżynierów o rezygnacji usługi montażusprzętu i odtworzenia systemów z kopii zapasowej.*

Sposób raportowania – zapisy
(odnośnie podjętych decyzji i działań z nich wynikających, itp.)

BIEŻĄCE ZAPISY W TRAKCIE TRWANIA ZDARZENIA
Dokonywane są w istniejącym systemie zarządzania zgłoszeniami (MAXIMO) jeżeli niemożliwe zapisy odręczne

ZAKOŃCZENIE DZIAŁAŃ
Dokonywane są w istniejącym systemie zarządzania zgłoszeniami (MAXIMO)

PRZEGLĄD I AKTUALIZACJI PLANU
Dokonywane są w istniejącym systemie zarządzania zgłoszeniami (MAXIMO)

ZAPISY I DOKUMENTY:

Testy i ćwiczenia
są przeprowadzane corocznie przed przeglądem systemu zarządzania przez Kierownictwo w kolejności:

1. *Przeprowadzenie próby DRP.*

NADZOROWANIE DOKUMENTU:

PRZEGLĄDY DOKUMENTU		
l.p.	Data przeglądu	Dokonujący przeglądu

Przegląd ustaleń zawartych w niniejszym Planie BCM oraz IMP przez Koordynatora ds. SZBI oraz odpowiedzialnych za poszczególne obszary powinien być realizowany:

A. Okresowo co 12 miesięcy wraz z przeglądem oceny ryzyka.
B. Każdorazowo po materializacji zagrożenia i uruchomieniu planu IMP i/lub BMC.
   W niniejszej sytuacji przegląd powinien dotyczyć:
   - Identyfikacji charakteru i przyczyn zdarzenia
   - Oceny adekwatności reakcji kierownictwa
   - Oceny skuteczności Organizacji w dotrzymaniu docelowego czasu wznowienia działalności
   - Oceny przydatności ustaleń związanych z BCM, które należy udoskonalić

   Przegląd powinien być udokumentowany w formie protokołu. Na podstawie stwierdzonych nieprawidłowości i zagrożeń oraz potencjałów do doskonalenia należy wprowadzić stosowane zmiany do niniejszego dokumentu oraz uruchomić stosowane działania zgodnie z procedurą PZ-06 Działania Korygujące i zapobiegawcze

KARTA ZMIAN			
l.p.	Podstawa	Treść zmiany	Uwagi

OPRACOWAŁ:	**ZATWIERDZIŁ:**
2013-02-12 **Maciej Miś** **Koordynator ds. SZBI**	

POLITYKA BEZPIECZEŃSTWA

Deklaracja

Zarząd Infomex Sp. z o.o. deklaruje zaangażowanie w prawidłowym zarządzaniu bezpieczeństwem informacji w Spółce. Oświadcza, iż dołoży wszelkich starań w celu zapewnienia bezpieczeństwa informacji, na poziomie uniemożliwiającym wykorzystanie, przepływ, modyfikację lub zniszczenia informacji w Spółce przez osoby postronne lub nieupoważnione a także na wypadek czynników zewnętrznych.

Dołoży wszelkich starań aby zapobiegać zdarzeniom dotyczącym bezpieczeństwa informacji a w przypadku ich wystąpienia odpowiednio reagować na nie w celu minimalizacji strat.

Szczegółowy zakres obowiązków i procedur postępowania w przypadku zagrożenia bezpieczeństwa informacji określone zostały w dokumentacji Zintegrowanego systemu Zarządzania Jakością i Bezpieczeństwem Informacji.

Zasady zarządzania bezpieczeństwem

1. Dane przetwarzane są w siedzibie Spółki Infomex Sp. z o.o. w Żywcu przy ul. Wesoła 19B.

2. Pomieszczenia firmy zabezpieczone są przed dostępem osób trzecich wydzielonymi strefami bezpieczeństwa oddzielonymi ścianami oraz przejściami pod kontrola Systemu Kontroli Dostępu.

3. Serwery znajdujące się w serwerowi firmy są chronione przed dostępem. Dostęp do nich posiada jedynie ograniczona liczba osób posiadająca odpowiedni poziom uprawnień, wynikający z wykonywanych zadań.

4. Dodatkowo pomieszczenia chronione są przez System Alarmowy i są pod stałym monitoringiem Systemu Telewizji Przemysłowej.

5. Nośniki informacji będącymi kopią bezpieczeństwa są przechowywane w strefie oddzielonej co najmniej dwoma przejściami i składowane w sejfie chronionym przed otwarciem kodem cyfrowym.

6. Dostęp z sieci publiczne do zasobów znajdujących się Spółce Infomex chronione są odpowiednimi fizycznymi i logicznymi zabezpieczeniami.

Procedura zarządzania aktualizacjami bezpieczeństwa

1. CEL

Celem niniejszej polityki jest opisanie polityk zarządzania infrastrukturą sprzętową oraz oprogramowaniem Systemu Informatycznego pod kontem instalacji poprawek bezpieczeństwa.

2. ZAKRES

Obowiązuje wszystkich pracowników firmy oraz osób wykonujących pracę w systemie informatycznym, których działania mogą mieć wpływ na bezpieczeństwo informacji w aspektach dostępności, poufności i integralności informacji.

3. DEFINICJE

System informatyczny - zespół współpracujących ze sobą urządzeń, systemów operacyjnych, oprogramowania biznesowego oraz narzędziowego, które stosowane są w systemie hostingowym ORE.

Użytkownik - osoba wykonujących pracę w systemie informatycznym, której nadano uprawnienia w zakresie oprogramowania jak i udostępnionego sprzętu (serwery, sieciowe urządzenia aktywne, aplikacje.)

4. Zarządzanie aktualizacjami oprogramowania oraz systemów operacyjnych

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa stasuje się następującą politykę dystrybucji poprawek bezpieczeństwa:

- Instalacja poprawek poprzedzona zostanie ich analizą w celu określenia wpływu na System Informatyczny oraz poziomu ważności dla danej poprawki.
- Jako poprawka *krytyczna* uznawana jest poprawka dla luki, której wykorzystanie może doprowadzić do wniknięcia kodu złośliwego bez udziału użytkownika.
- Jako poprawka *ważna* uznawana jest poprawka dla luki, której wykorzystanie może doprowadzić do naruszenia poufności, integralności lub dostępności danych użytkownika lub do naruszenia integralności bądź dostępności zasobów przetwarzania.
- Jako poprawka *umiarkowana* uznawana jest poprawka dla luki , której wykorzystanie jest w znacznym stopniu ograniczone przez konfigurację lub jest trudna do wykorzystania.
- Jako poprawka *niska* uważana jest luka, której wykorzystanie jest niezwykle trudne lub, której znaczenie jest minimalne.
- Wykonanie testowej instalacji poprawek przed wdrożeniem ich w systemie produkcyjnym.
- Poprawki dla serwerów będą dystrybuowane po godzinie 16:00.
- Poprawki krytyczne oraz ważne dystrybuowane będą najpóźniej w tygodniowym odstępie od daty ukazania się informacji o niej i po wykonaniu instalacji w środowisku testowym.

Procedura zarządzania dostępem do systemów informatycznych

1. CEL

Celem niniejszej polityki jest opisanie zasad nadawania uprawnień użytkownikom oraz zasad dotyczących korzystania z systemów informatycznych działających w sieci LAN.

2. ZAKRES

Instrukcja dla użytkowników, odpowiedzialnych za administrowanie systemów informatycznych.

3. DEFINICJE

Administrator systemu informatycznego - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego.

System informatyczny - zespół współpracujących ze sobą urządzeń, systemów operacyjnych, oprogramowania biznesowego oraz narzędziowego, które stosowane są w systemie hostingowym ORE.

Bezpieczeństwo systemu informatycznego - wdrożone środki i rozwiązania techniczne oraz oprogramowanie w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.

Użytkownik systemu - osoba posiadająca uprawnienia do przetwarzania informacji w systemie informatycznym. Posiadająca unikalny identyfikator konta użytkownika i unikalne znane tylko sobie hasło.

Maximo – Oprogramowanie IBM SmartCloud Control Desk, kompleksowe rozwiązanie do zarządzania zasobami i usługami informatycznymi, które posiada zautomatyzowaną obsłudze zgłoszeń serwisowych, zarządzaniu zmianami oraz optymalizacji zarządzania cyklem życia zasobów informatycznych.

Microsoft Active Directory – System umożliwiający centralne zarządzanie tożsamościami, relacjami w sieci firmowej, umożliwia kontrolę nad siecią i zasobami w niej działającymi. W usłudze Active Directory są tworzone konta użytkowników oraz komputerów.

4. NADAWANIE ODBIERANIE UPRAWNIEŃ UŻYTKOWNIKOM

Nadanie Uprawnień do systemu informatycznego polega na przyznaniu unikalnego identyfikatora. Konieczność nadania uprawnień każdorazowo rejestrowane jest w systemie Maximo. Zlecenie utworzenia nowego użytkownika powinno zawierać następujące informacje:

- Imię i nazwisko,
- Stanowisko jakie będzie pełnione oraz dział firmy,
- Miejsce w jakim będzie świadczona praca,
- Nazwy systemów informatycznych do których zostaną nadane uprawnienia, poza z góry ustalony zakres uprawnień standardowych.
- Datę z jaką uprawnienia ma być nadane.

Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada administrator odpowiedniego systemu informatycznego.

Odbieranie Uprawnień do systemu informatycznego wykonywane jest każdorazowo po zarejestrowaniu rekordu w systemie Maximo. Uprawnienia są odbierane w momencie zmiany stanowiska lub zwolnienia pracownika.

5. POLITYKA NADAWANIA UPRAWNIEŃ

Dostęp do danych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał. Identyfikator oraz hasło powinno spełniać następujące warunki:

- Identyfikator użytkownika składa się inicjałów użytkownika, znaki identyfikatora nie są rozdzielone spacjami nie zawierają polskich znaków
- Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika

  z systemu informatycznego nie może być przydzielany innej osobie.
- Identyfikator przypisany użytkownikowi powinien być stosowany do autoryzacji we wszystkich systemach, urządzeniach oraz oprogramowaniu działającym w obrębie systemu informatycznego
- Minimalna długość hasła wynosi 8 znaków,
- Hasło powinno być unikalne
- Hasło musi składać się z małych i wielkich liter i co najmniej jednej cyfry. Hasło nie może zawierać liter powtarzających więcej niż dwa razy (np. stosowanie hasła „aabbbaa1” jest niedopuszczalne). Hasło nie może zawierać następujących wyrazów : twojego imienia, nazwiska, nazwy komputera.

Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym, posiadają odpowiedni poziom uprawnień dla swoich kont. Poziom uprawnień nadawany jest zgodnie z wykonywanymi czynnościami administracyjnymi nie wykraczającymi poza zakres kompetencji. Poza odpowiednim poziomem uprawnień, osoby uprawnione posiadają konta administracyjne do urządzeń i systemów działających poza kontrolą Microsoft Active Directory, do których mają przydzielone hasło. Zasady zarządzania hasłami są analogiczne, jak w przypadku haseł użytkowników. Nazwy i hasła użytkowników posiadających uprawnienia administratorów systemów informatycznych przechowywane są w zamkniętej szafie, która znajduje się w zabezpieczonej Strefie Bezpieczeństwa. Nazwy użytkowników oraz hasła powinny być przechowywane w opieczętowanej kopercie.

W przypadku konieczności awaryjnego użycia nazw i haseł tych użytkowników konieczny jest wpis ilustrujący zaistniała sytuację w „Dzienniku użycia" znajdującym się w szafie wraz z kopertą, w której znajdują się hasła. Wpis powinien zawierać następujące informacje:

- Datę i godzinę otwarcia koperty
- Imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
- Krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

Procedura zarządzania incydentem bezpieczeństwa

1. CEL

Celem procedury jest zapewnienie odpowiedniego postępowania na wypadek wystąpienia zdarzenia lub incydentu związanego z Bezpieczeństwem Informacji.

2. ZAKRES STOSOWANIA

a. Zakres podmiotowy

Instrukcja obowiązuje wszystkich pracowników.

b. Zakres przedmiotowy

Instrukcja obowiązuje w przypadku wystąpienia incydentu lub zdarzenia związanego z bezpieczeństwem informacji, które mogą mieć miejsce w każdym z realizowanych przez firmę procesów lub działań.

3. DEFINICJE

System informatyczny - zespół współpracujących ze sobą urządzeń, systemów operacyjnych, oprogramowania biznesowego oraz narzędziowego, które stosowane są w systemie hostingowym ORE.

Zdarzenie - zdarzenie związane z bezpieczeństwem informacji jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem. Zdarzenie to potencjalny incydent.

Incydent – incydent związany z bezpieczeństwem informacji jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji

4. ODPOWIEDZIALNOŚĆ

4.1 Koordynator BI odpowiada za:

- Nadzór nad stosowaniem niniejszej instrukcji w obszarze całego systemu zarządzania
- Okresowe przeglądy danych i informacji dotyczących mających miejsce w danym okresie zdarzeń i incydentów dotyczących bezpieczeństwa informacji
- Przygotowywanie niezbędnych danych dotyczących zdarzeń i incydentów BI dla kierownictwa

4.2 Odpowiedzialny za dany obszar (oddział, proces) odpowiada za:

4.2.1 Zapewnienie odpowiedniej świadomości podległych sobie pracowników oraz nadzorowanych przez siebie osób wykonujących pracę dla lub na rzecz Organizacji dotyczącej postępowania ze zdarzeniami i incydentami

4.3 Pracownicy działu technicznego odpowiada za:

4.3.1 Analiza zdarzeń i incydentów zgłaszanych przez podległych pracowników oraz dokumentowanie wyników analiz w systemie informatycznym oraz uruchamianie stosownych działań naprawczych (incydenty)

4.3.2 Uruchamianie działań zapobiegawczych (zdarzenia) oraz korygujących (incydenty) w stosunku do zgłaszanych zdarzeń i incydentów przez pracowników, osób współpracujących, Klientów i innych stron zainteresowanych
Komunikację z Koordynatorem w zakresie postępowania ze zdarzeniami i incydentami

4.3.3 Natychmiastową reakcję na zdarzenie lub incydent, w ramach zakresu swoich kompetencji, w celu zminimalizowania prawdopodobieństwa wystąpienia danego zdarzenia /incydentu (działanie proaktywne) lub w celu zminimalizowania potencjalnych lub rzeczywistych skutków zdarzenia /incydentu

4.3.4 Zgłaszanie w systemie wszelkich zdarzeń dotyczących Bezpieczeństwa Informacji które mogły zakończyć się incydentem (konsekwencjami dla firmy w zakresie bezpieczeństwa informacji) (ZDARZENIE)

4.3.5 Zgłaszanie w systemie wszelkich zidentyfikowanych incydentów dotyczących Bezpieczeństwa Informacji (INCYDENT)

4.4 Klient odpowiadają za**:**

4.4.1 Zgłaszanie do osób odpowiedzialnych za kontakt z nimi lub operatora monitoringu wszelkich dostrzeżonych zdarzeń lub incydentów dotyczących bezpieczeństwa informacji związanych z realizowaną dla nich usługą lub w ramach realizowanych przez firmę procesów z którymi mają do czynienia.

Raport wdrożeniowy aplikacji epodreczniki.pl

Spis treści:

1. Analiza dokumentacji

Zapoznanie się z dokumentacją administracyjno-programistyczną oraz dokumentacją architektury platformy technologicznej oraz innymi dostarczonymi dokumentami.

2. Przygotowanie serwerów

Utworzenie maszyn wirtualnych wraz z odpowiednimi systemami operacyjnymi, aktualizacja i konfiguracja systemów operacyjnych, sieci, tworzenie kont dostępowych dla administratorów i programistów.

3. Instalacja oprogramowania i usług

Instalacja i konfiguracja wymaganego oprogramowania zgodnie z dokumentacją instalacji i doświadczeniem administratorów oraz programistów Infomex.

4. Wgranie kopii zapasowej

Wgranie dostarczonej kopii zapasowej na właściwe serwery i konfiguracja usług do ich poprawnego użycia.

5. Konfiguracja usług dodatkowych

Konfiguracja równoważenia obciążenia sieciowego, routera, VPN, firewall, IPS, kopii zapasowych, monitoringu serwerów i usług oraz systemu helpdeskowego.

6. Zmiany w DNS

Zmiana w rekordach serwera nazw domeny epodreczniki.pl, przepięcie ruchu z Internetu na serwery Infomex.