UCHWAŁA ZARZĄDU NR 43/X/2025
Śląskiego Fundusz Rozwoju Sp. z o.o.
z dnia 21 października 2025 roku

w sprawie: wprowadzenia Księgi procesów i procedur IT w zakresie zarzadzania bezpieczeństwem informacji

Działając na podstawie § 31 ust .1 Aktu Założycielskiego Śląskiego Funduszu Rozwoju Sp. z o.o., Zarząd uchwala:

§ 1

Przyjmuje się i wprowadza do stosowania przez wszystkie komórki organizacyjne w Spółce/ Pracowników Spółki/samodzielne stanowiska dokument pn.„Księga procesów i procedur IT w zakresie zarządzania bezpieczeństwem informacji".

§ 2

Nadzór nad prawidłową realizacją Uchwały powierza się Panu Tomaszowi Kazimierczakowi – Administratorowi Systemów Informatycznych Spółki

§ 3

Niniejsza Uchwała wchodzi w życie z dniem podjęcia.

Uchwała została podjęta następującymi głosami:

„za"	1
„przeciw"	0
„wstrzymujących się"	0

Podpis
- Prezes Zarządu Joanna Schmid

30 WRZEŚNIA 2025

PROCESY I PROCEDURY IT

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

TOMASZ KAŹMIERCZAK

Tomasz Kaźmierczak

Specjalista ds. Informatyki

Spis treści

Tomasz Kaźmierczak

Specjalista ds. Informatyki

1. Cel dokumentu

Celem niniejszego dokumentu jest przeprowadzenie inwentaryzacji, analizy zasobów informatycznych oraz opisanie procesów i procedur związanych z ich utrzymaniem i bezpieczeństwem. Dokument ma na celu:

- przedstawienie aktualnego stanu infrastruktury IT
- opisanie procesów operacyjnych oraz procedur awaryjnych obowiązujących w Spółce
- wskazanie obowiązujących polityk bezpieczeństwa i zasad dostępu
- identyfikację potencjalnych ryzyk związanych z funkcjonowaniem systemów IT
- zapewnienie spójnego zestawu wytycznych dla administratorów i użytkowników, co ma służyć zwiększeniu poziomu bezpieczeństwa, ciągłości działania oraz zgodności z najlepszymi praktykami

Dokument stanowi podstawę do dalszych działań w zakresie doskonalenia infrastruktury IT, podnoszenia bezpieczeństwa oraz wdrażania procedur ograniczających ryzyko związane z incydentami informatycznymi.

Zakres niniejszego dokumentu obejmuje:

- inwentaryzację sprzętu komputerowego, serwerów, urządzeń sieciowych oraz peryferyjnych,
- wykaz usług zewnętrznych wykorzystywanych przez Spółkę,
- zestawienie oprogramowania, w tym systemów operacyjnych i aplikacji krytycznych,
- opis procesów związanych z zarządzaniem użytkownikami, backupem, aktualizacjami oraz dostępem do zasobów,
- procedury awaryjne i sposób postępowania w przypadku wystąpienia incydentów,
- polityki bezpieczeństwa obowiązujące w organizacji,
- analizę ryzyka.

Dokument nie obejmuje:

- szczegółowych konfiguracji technicznych poszczególnych urządzeń i systemów,
- dokumentacji projektowej dotyczącej rozwoju infrastruktury,
- aspektów finansowych związanych z utrzymaniem i rozbudową systemów IT.

2. Inwentaryzacja zasobów

Niniejszy rozdział opisuje zasoby IT wykorzystywane w Spółce. Celem inwentaryzacji jest zapewnienie pełnej widoczności zasobów.

Inwentaryzacja jest dokumentem żywym, aktualizowanym po każdej istotnej zmianie oraz przeglądanym co najmniej raz na rok.

2.1 Sprzęt

Sekcja obejmuje wszystkie fizyczne elementy infrastruktury IT. Sprzęt opisany w podrozdziałach stanowi aktualny stan środowiska produkcyjnego wraz z komponentami zapasowymi.

2.1.1 – Forti Gate 40F

Urządzenie FortiGate, z aktywną licencją producenta, pełni funkcję głównej bramy bezpieczeństwa w infrastrukturze sieci. Zostało do niego doprowadzone redundantne połączenie z dwoma niezależnymi łączami internetowymi, zapewnianymi w ramach usługi dostępu do sieci świadczonej przez Ekoenergia Silesia. Na urządzeniu FortiGate w Security Profiles włączone zostały mechanizmy ochronne:

AntyVirus – skanowanie ruchu sieciowego w celu wykrywania i blokowania złośliwego oprogramowania.

Web Filter – kontrola dostępu do stron internetowych według kategorii lub adresów URL.

DNS Filter – filtrowanie zapytań DNS i blokowanie połączeń do szkodliwych lub niepożądanych domen.

Application Control – identyfikacja i kontrola aplikacji w ruchu sieciowym

IPS – wykrywanie i blokowanie prób ataków sieciowych oraz exploitów.

SSL Inspection – inspekcja szyfrowanego ruchu (HTTPS), aby inne profile bezpieczeństwa mogły działać także na zaszyfrowanych danych.

2.1.2 – Forti Gate 30E

Poprzednio wykorzystywane urządzenie FortiGate zostało zastąpione modelem FortiGate 40F ze względu na brak możliwości dalszego odnawiania licencji. Obecnie pełni ono rolę urządzenia rezerwowego, przeznaczonego do wykorzystania w przypadku fizycznej awarii aktywnego urządzenia FortiGate 40F.

Tomasz Kaźmierczak

Specjalista ds. Informatyki

2.1.3 – Serwer Plików Synology DS224+

Serwer plików Synology DS224+ pełni funkcję centralnego systemu kopii zapasowych. Codziennie wykonywane są automatyczne kopie zapasowe wszystkich laptopów będących w posiadaniu spółki. W przypadku awarii stacji roboczej, dane użytkownika pozostają zabezpieczone i dostępne na serwerze plików. System przechowuje kopie z ostatnich 10 udanych cykli backupowych, zapewniając możliwość odtworzenia plików z wcześniejszych dni pracy.

2.1.4 – Serwer Plików Synology RS819

Serwer plików wykorzystywany jest jako centralne repozytorium dokumentów archiwalnych oraz przestrzeń robocza dla pracowników Spółki, udostępniana w formie udziału sieciowego. Dodatkowo z zasobu wspólnego wykonywana jest regularna kopia zapasowa, która przechowywana jest na serwerze plików Synology DS224+

2.1.5 – Drukarka C250i

Podstawowe urządzenie drukujące-skanujące w Spółce. Wszystkie komputery firmowe posiadają możliwość korzystania z drukarki. Urządzenie zapewnia druk dwustronny oraz skanowanie przy użyciu dwóch modułów: skanera płaskiego (tradycyjnego) oraz skanera z automatycznym podajnikiem dokumentów.

2.1.6 – Drukarka C454e

Starsze urządzenie drukujące, zastąpione nowszym modelem C250i. Obecnie pełni funkcję zapasowego skanera. Moduł skanera płaskiego oraz automatyczny podajnik dokumentów pozostają w pełni sprawne i są wykorzystywane w razie potrzeby.

2.1.7 – Przełącznik TP-Link

Główny przełącznik sieciowy Spółki, do którego podłączone są wszystkie urządzenia aktywne oraz końcowe w infrastrukturze sieciowej. Odpowiada za dystrybucję ruchu sieciowego pomiędzy serwerami, stacjami roboczymi, urządzeniami peryferyjnymi oraz punktami dostępowymi Wi-Fi.

2.1.8 - FortiAP oraz Ubiquiti

Urządzenia sieciowe zapewniające bezprzewodowy dostęp do sieci firmowej. Zostały rozmieszczone w taki sposób, aby zapewnić pełne pokrycie sygnałem Wi-Fi wszystkich pomieszczeń użytkowanych przez pracowników Spółki. Aktualnie Spółka dysponuje 3 sztukami FortiAP oraz 1 sztuką Ubiquiti.

2.2 Usługi zewnętrzne

Sekcja obejmuje usługi świadczone przez podmioty trzeci

2.2.1 – Hosting AZ.pl

Spółka korzysta z usług hostingowych dostarczanych przez AZ.pl. Na serwerze zlokalizowane są główne usługi poczty elektronicznej, serwisy internetowe oraz bazy danych.

2.2.2 – Hosting Webd.pl

Spółka posiada wykupiony hosting w Webd.pl, na którym uruchomione są kluczowe aplikacje. Środowisko zarządzane jest poprzez panel administracyjny cPanel, co umożliwia sprawne zarządzanie usługami hostingowymi, pocztą oraz bazami danych. Dodatkowo hosting pełni funkcję zapasową dla serwera pocztowego, zapewniając ciągłość działania w przypadku awarii głównej usługi.

2.2.3 – VPS w SeoHost

Spółka dysponuje serwerem wirtualnym (VPS) w SeoHost, na którym zainstalowany i utrzymywany jest system PBAZA

2.2.4 – Hosting OVH

W ramach usług OVH Spółka posiada wykupione domeny internetowe siecrozwoju.pl oraz siecrozwoju.eu. Umowy rejestracyjne zostały zawarte na okres 10 lat, co zapewnia stabilność oraz długoterminowe zabezpieczenie praw do nazw domenowych.

Tomasz Kaźmierczak

Specjalista ds. Informatyki

2.2.5 – Comarch Optima

Spółka posiada wykupione dwie licencje oprogramowania Comarch Optima w module Kadrowo–Finansowo–Księgowym. System ten wspiera procesy księgowe, kadrowe oraz finansowe, stanowiąc istotny element infrastruktury informatycznej Spółki.

2.3 Serwisy internetowe

Opis poniżej przedstawia utrzymywane przez Spółkę serwisy i aplikacje internetowe wraz z podstawowymi informacjami o technologii.

2.3.1 – sfr-slaskie.pl

- Opis: Główna strona internetowa Spółki, zawierająca informacje o działalności Spółki
- Technologia: WordPress
- Hosting: AZ.pl.
- Bezpieczeństwo: Certyfikat SSL (Let's Encrypt) odnawiany co rok, kopie zapasowe wykonywane w ramach hostingu az.pl oraz ręcznie wykonywane kopie zapasowe przez FTP na Serwer Plików Synology DS224+
- Administracja: Tomasz Kaźmierczak.

2.3.2 – bip.sfr-slaskie.pl

- Opis: Biuletyn Informacji Publicznej prowadzony w ramach obowiązków ustawowych.
- Technologia: Joomla.
- Hosting: AZ.pl.
- Bezpieczeństwo: Certyfikat SSL (Let's Encrypt) odnawiany co rok, kopie zapasowe wykonywane w ramach hostingu az.pl oraz ręcznie wykonywane kopie zapasowe przez FTP na Serwer Plików Synology DS224+
- Administracja: Tomasz Kaźmierczak we współpracy z sekretariatem.

2.3.3 – efp-slaskie.pl

- Opis: Archiwalna strona projektu EFP, utrzymywana w celach dokumentacyjnych, strona opisująca wydarzenie EFP z 6-8 październik 2021
- Technologia: WordPress
- Hosting: AZ.pl.
- Bezpieczeństwo: W uwagi na utrzymywanie w celach dokumentacyjnych, kopia zapasowa przechowywana jest również lokalnie na serwerze plików.
- Administracja: Tomasz Kaźmierczak

2.3.4 – slaskifunduszrozwoju.pl

- Opis: Domena główna wykorzystywana do obsługi serwisów i aplikacji Spółki. Pełni funkcję centralnej domeny, w ramach której tworzone są subdomeny dla poszczególnych systemów (m.in. raportowanie, pożyczki, rejestracja czasu pracy).
- Administracja: Tomasz Kaźmierczak

2.3.4.1 – raport.slaskifunduszrozwoju.pl

- Opis: System raportowy dla pośredników finansowych umożliwiający składanie sprawozdań online.
- Technologia: Dedykowana aplikacja napisana i wdrożona przez Tomasza Kaźmierczaka.
- Hosting: Webd.pl
- Bezpieczeństwo: Certyfikat SSL aktywny, regularne kopie zapasowe.
- Administracja: Tomasz Kaźmierczak

2.3.4.2 – pozyczki.slaskifunduszrozwoju.pl

- Opis: Serwis powiązany z systemem PBaza, z którego korzystają pracownicy Spółki.
- Technologia: Dedykowana aplikacja (PBaza).
- Hosting: VPS w SeoHost.
- Bezpieczeństwo: Certyfikat SSL aktywny, backup bazy oraz wszystkich plików wykonywany manualnie.
- Administracja: Tomasz Kaźmierczak ze współpracy z twórcami programu PBaza

2.3.4.3 – rcp.slaskifunduszrozwoju.pl

- Opis: System rejestracji czasu pracy dla pracowników pracujących zdalnie.
- Technologia: Dedykowana aplikacja RCP napisana i wdrożona przez Tomasza Kaźmierczaka
- Hosting: Webd.pl
- Bezpieczeństwo: Certyfikat SSL (Let's Encrypt) odnawiany automatycznie., ograniczony dostęp do aplikacji (tylko użytkownicy Spółki pracujący zdalnie)
- Administracja: Dział IT Spółki.

2.4 Oprogramowanie

Niniejsza sekcja obejmuje oprogramowanie instalowane i używane w Spółce

2.4.1 – Oprogramowanie antywirusowe ESET

- Zakres: Zainstalowane na wszystkich komputerach firmowych.
- Funkcje: Ochrona przed złośliwym oprogramowaniem, phishingiem i innymi zagrożeniami sieciowymi.
- Aktualizacje: Definicje wirusów i silnik skanowania aktualizowane automatycznie
- Polityka skanowania: Skanowanie w czasie rzeczywistym
- Administrator techniczny: Tomasz Kaźmierczak

Tomasz Kaźmierczak

Specjalista ds. Informatyki

2.4.2 – Oprogramowanie biurowe Microsoft Office

- Zakres: Zainstalowane na wszystkich komputerach należących do Spółki; służy do pracy z dokumentami, arkuszami kalkulacyjnymi i prezentacjami.
- Licencjonowanie: Konta licencyjne przypisywane do użytkowników w ramach konta pocztowego office(5 ostatnich znaków klucza licencyjnego)@sfr-slaskie.pl

  Przykład: jeśli klucz licencyjny zawiera fragment 12345-abcde-abc123, przypisany adres licencyjny: abc123@sfr-slaskie.pl.
- Aktualizacje: Aktualizacje automatyczne według dostępności
- Kopie zapasowe dokumentów: Realizowane w ramach serwera plików DS224+

Administrator techniczny: Dział IT.

3. Opis procesów

Celem niniejszego rozdziału jest zdefiniowanie standardowych sposobów działania

3.1 Zarządzanie użytkownikami

Celem zarządzania użytkownikami jest zapewnienie, że dostęp do zasobów Spółki jest nadawany, zmieniany i odbierany w sposób kontrolowany, zgodny z zasadą najmniejszych uprawnień oraz wymaganiami bezpieczeństwa.

3.1.1 – Zarządzanie użytkownikami na komputerach

Każdy pracownik posiada dwa hasła:

- pierwsze służące do odszyfrowania dysku komputera,
- drugie służące do logowania się na konto użytkownika w systemie operacyjnym.

Konta tworzone są przez Administratora po otrzymaniu informacji o przyjęciu nowego pracownika. Uprawnienia nadawane są zgodnie z zakresem obowiązków i ustaleniami przełożonych.

3.1.2 – Zarządzanie użytkownikami na serwerach plików

- Opis: każdy pracownik otrzymuje indywidualne konto na serwerze plików. Konta te wykorzystywane są zarówno do wykonywania cyklicznych kopii zapasowych danych użytkowników, jak i do przydzielania dostępu do wspólnych folderów działowych.
- Przyznawanie dostępu: zakres uprawnień ustalany jest na podstawie wytycznych kierowników poszczególnych działów.
- Dostęp: możliwość logowania jest ściśle ograniczona do sieci wewnętrznej Spółki.

3.1.3 – Zarządzanie użytkownikami w systemie RCP (Rejestr Czasu Pracy)

- Opis: każdy pracownik posiada unikalny numer identyfikacyjny, który jest wymagany do logowania w systemie RCP. System nie przechowuje żadnych danych osobowych. Zapisuje wyłącznie numer identyfikacyjny, który jest dekodowany lokalnie. Na jego podstawie generowana jest lista obecności. Rozwiązanie to zapewnia zgodność z zasadami ochrony danych osobowych, minimalizując zakres gromadzonych informacji.
- Przyznawanie dostępu: konta tworzone są na podstawie decyzji przełożonych.
- Dostęp: uprawnienia ograniczone są wyłącznie do osób wskazanych przez przełożonych.

3.1.4 – Zarządzanie użytkownikami w systemie PBAZA

- Opis: użytkownicy systemu PBAZA logują się za pomocą indywidualnych loginów oraz haseł.
- Przyznawanie dostępu: konta przyznawane są na podstawie decyzji przełożonych.
- Dostęp: uprawnienia ograniczone są wyłącznie do osób wskazanych przez przełożonych.

3.1.5 – Zarządzanie użytkownikami w systemie RAPORT

- Opis: Dostęp do systemu posiadają pośrednicy finansowi oraz wybrani pracownicy Spółki. Każdy użytkownik dysponuje dwoma kontami:
  - pierwszym umożliwiającym wyświetlenie systemu,
  - drugim służącym do pełnego logowania i korzystania z aplikacji.
- Przyznawanie dostępu: Konta wydawane są na podstawie polecenia przełożonych.
- Dostęp: Uprawnienia ograniczone są wyłącznie do osób wskazanych przez przełożonych.

3.2 Backup i odtwarzanie danych

3.2.1 – strona internetowa sfr-slaskie.pl

Zakres

- Polityka obejmuje kopie zapasowe plików serwisu oraz powiązanej bazy danych.

Model backupu

- Backup w ramach hostingu (az.pl): kopia pełna wykonywana automatycznie przez dostawcę hostingu i obejmuje pliki strony oraz bazę danych.
- Backup manualny (wewnętrzny) dodatkowa kopia realizowana przez Pracownika IT

Harmonogram

- Hosting (az.pl): wykonywanie codziennie.
- Manualny: wykonywanie raz w tygodniu.

Tomasz Kaźmierczak

Specjalista ds. Informatyki

Retencja

- Hosting (az.pl): przechowywanie kopii przez 3 dni.
- Manualny: przechowywanie kopii przez 3 miesiące.

3.2.2 – strona internetowa bip.sfr-slaskie.pl

Zakres

- Polityka obejmuje kopie zapasowe plików serwisu oraz powiązanej bazy danych.

Model backupu

- Backup w ramach hostingu (az.pl): kopia pełna wykonywana automatycznie przez dostawcę hostingu i obejmuje pliki strony oraz bazę danych.
- Backup manualny (wewnętrzny): dodatkowa kopia realizowana przez Pracownika IT.

Harmonogram

- Hosting (az.pl): wykonywanie codziennie.
- Manualny: wykonywanie raz w tygodniu.

Retencja

- Hosting (az.pl): przechowywanie kopii przez 3 dni.
- Manualny: przechowywanie kopii przez 3 miesiące.

3.2.3 – aplikacja raport

Zakres

- Polityka obejmuje kopie zapasowe plików serwisu oraz powiązanej bazy danych.

Model backupu

- Backup w ramach hostingu (webd.pl): kopia pełna wykonywana automatycznie przez dostawcę hostingu i obejmuje pliki strony oraz bazę danych.
- Backup manualny (wewnętrzny): dodatkowa kopia realizowana przez Pracownika IT.

Harmonogram

- Hosting (webd.pl): wykonywanie codziennie.
- Manualny: wykonywanie raz w tygodniu.

Retencja

- Hosting (webd.pl): przechowywanie kopii przez 14 dni.
- Manualny: przechowywanie kopii przez 3 miesiące.

3.2.4 – aplikacja PBAZA

Zakres

- Polityka obejmuje kopie zapasowe plików serwisu oraz powiązanej bazy danych.

Model backupu

- Backup manualny (wewnętrzny): kopia realizowana przez Pracownika IT

Harmonogram

- Manualny: wykonywanie dwa razy w tygodniu

Retencja

- Manualny: przechowywanie kopii przez 3 miesiące.

3.2.5 – poczta sfr-slaskie.pl

Zakres
Polityka obejmuje kopie zapasowe plików poczty @sfr-slaskie.pl

Model backupu

- Backup w ramach hostingu (az.pl): kopia pełna wykonywana automatycznie przez dostawcę hostingu.
- Backup manualny (wewnętrzny): dodatkowa kopia realizowana przez Pracownika IT

Harmonogram

- Hosting (az.pl): wykonywanie codziennie.
- Manualny: wykonywanie raz w tygodniu – tylko skrzynki funkcyjne.

Retencja

- Hosting (az.pl): przechowywanie kopii przez 3 dni.
- Manualny: przechowywanie kopii przez 3 miesiące - tylko skrzynki funkcyjne.

3.2.3 – rejestrator czasu pracy

Zakres
Polityka obejmuje kopie zapasowe plików serwisu oraz powiązanej bazy danych.

Model backupu

- Backup w ramach hostingu (webd.pl): kopia pełna wykonywana automatycznie przez dostawcę hostingu i obejmuje pliki strony oraz bazę danych.

Tomasz Kaźmierczak

Specjalista ds. Informatyki

- Backup manualny (wewnętrzny): dodatkowa kopia realizowana przez Pracownika IT

Harmonogram

- Hosting (webd.pl): wykonywanie codziennie.
- Manualny: wykonywanie raz na miesiąc

Retencja

- Hosting (webd.pl): przechowywanie kopii przez 14 dni.
- Manualny: przechowywanie kopii przez 3 miesiące.

3.3 Aktualizacje i łatki bezpieczeństwa

Utrzymanie wysokiego poziomu bezpieczeństwa i stabilności poprzez terminowe wdrażanie poprawek systemowych i aplikacyjnych.

3.3.1 Systemy stacji roboczych (Windows)

- Tryb wdrażania: Automatyczny. Aktualizacje systemu Windows są instalowane podczas wyłączania komputera przez użytkownika.
- Wymóg eksploatacyjny: użytkownik powinien co najmniej raz w tygodniu wykonać pełne wyłączenie systemu i aktualizację jeżeli jest dostępna.
- Restart: jeśli wymagany, następuje po instalacji aktualizacji przy wyłączaniu lub przy następnym uruchomieniu.

3.3.2 Oprogramowanie antywirusowe

- Tryb wdrażania: Automatyczny. Instalowane automatycznie podczas pracy komputera.
- Polityka: w razie wykrycia krytycznej luki producenta, Pracownik IT może wymusić wcześniejszą instalację poza standardowym cyklem.
- Restart: jeśli wymagany, następuje po instalacji aktualizacji.

3.3.3 Aplikacja PBAZA

- Model utrzymania: aktualizacje wykonywane wraz z pomocą techniczną producenta PBAZA.
- Procedura: przed aktualizacją wykonywana jest kopia bazy i plików.
  Po aktualizacji przeprowadzane są testy funkcjonalne kluczowych scenariuszy.
- Okno serwisowe: uzgadniane z właścicielem systemu oraz pracowników Spółki.

3.3.4 Zapora FortiGate

- Model utrzymania: aktualizacje oprogramowania/firmware'u realizowane są wraz z pomocą techniczną firmy NBIT (świadczenie w cenie zakupu urządzenia).
- Procedura: przed aktualizacją wykonywana jest kopia konfiguracji

- Okno serwisowe: planowane i komunikowane z wyprzedzeniem

3.4 Dostęp fizyczny

Cel: Ochrona infrastruktury IT poprzez kontrolę i rejestrację dostępu do pomieszczeń oraz nośników.

3.4.1 Serwerownia i szafa rack

- Lokalizacja i zabezpieczenia: serwerownia oraz szafa rack jest zamykana na klucz
- Uprawnieni do wejścia: Pracownicy Ekoenergii oraz Tomasz Kaźmierczak.
- Zasady pracy: drzwi serwerowni pozostają zamknięte a wejście możliwe wyłącznie dla osób uprawnionych. Przebywanie osób trzecich wymaga asysty osoby uprawnionej.

3.4.2 Zarządzanie kluczami i kontrola wejść do siedziby

- Pobieranie kluczy: dostęp do pomieszczeń Spółki odbywa się poprzez pobranie klucza w recepcji z elektrycznej szafki na klucze, otwieranej kartą pracowniczą.
- Procedura dzienna:
    - Pierwsza osoba uprawniona pobiera klucz i otwiera pomieszczenia.
    - Ostatnia osoba zwraca klucz do szafki i zamyka drzwi na klucz.
- Stan drzwi w trakcie dnia: drzwi są zamknięte, a otwarcie możliwe wyłącznie kartą.

3.4.3 Zasady dla gości i wykonawców

- Wejście wyłącznie po wcześniejszym zgłoszeniu
- Pobyt w strefach technicznych wyłącznie pod nadzorem osoby uprawnionej.

3.4.4 Utrata karty lub klucza dostępu

- Utrata/kradzież karty lub klucza zgłaszana jest niezwłocznie i karta jest blokowana a zamki w razie potrzeby wymienione.

4. Procedury awaryjne

Celem procedur awaryjnych jest szybkie ograniczenie skutków zdarzeń, odtworzenie działania usług do akceptowalnego poziomu

4.1 Brak dostępu do Internetu

Urządzenie FortiGate 30E jest skonfigurowane do automatycznego przełączania na łącze zapasowe w przypadku niedostępności łącza podstawowego.

Działanie:

- Przełączenie odbywa się automatycznie; użytkownik końcowy nie wykonuje żadnych czynności.

Tomasz Kaźmierczak

Specjalista ds. Informatyki

4.2 Brak zasilania

Urządzenia sieciowe są podłączone do zasilacza awaryjnego (UPS), który zapewnia podtrzymanie pracy przez ok. 30 minut.

Działania:

- Pracownicy korzystający z laptopów kontynuują pracę na zasilaniu bateryjnym.
- W razie przedłużającej się przerwy w dostawie prądu – bezpieczne zapisanie dokumentów i wylogowanie z systemów.

4.3 Awaria zapory FortiGate 40F

Niezdolność do pracy urządzenia FortiGate 40F.

Działania:

- Przełączyć ruch na zapasowe urządzenie FortiGate 30E.
- Okablowanie wpiąć w identycznej kolejności jak w FortiGate 40F.

4.4 Awaria punktu dostępowego (Wi-Fi)

W przypadku awarii AP spółką posiada zapasowy AP który należy wymienić w miejscu uszkodzonego. Wszystkie AP są zasilane POE oraz są skonfigurowane

Działanie:

- Wymienić uszkodzony AP na zapasowy znajdujący się w zasobach Spółki.
- Wszystkie AP są zasilane w standardzie POE oraz są wstępnie skonfigurowane do pracy w bieżącej infrastrukturze.

4.5 Awaria Dysku na Synology DS224+

Urządzenie wyposażone jest w dwa dyski pracujące w konfiguracji lustrzanej, zapewniającej tolerancję awarii jednego nośnika.

Działania:

- Niezwłocznie wymienić uszkodzony dysk na nowy o identycznych parametrach (pojemność, interfejs, klasa).

4.6 Awaria Dysku Synology RS819

Urządzenie posiada cztery dyski i jest skonfigurowane z tolerancją awarii jednego nośnika.

Działania:

- Niezwłocznie wymienić uszkodzony dysk na nowy o identycznych parametrach.

4.7 Awaria Drukarki

Opis: Drukarka jest objęta umową dzierżawy i serwisem.

Działanie:

- Niezwłocznie zgłosić awarię do serwisu.
- W razie potrzeby skanowania dokumentów – skorzystać z drugiej dostępnej w Spółce drukarki ze sprawnym skanerem.

4.8 Awaria Laptopa

Opis: Niezdolność użytkownika do pracy na dotychczasowym urządzeniu.
Działania:

- Odzyskać dane użytkownika z kopii zapasowej przechowywanej na DS224+.
- Wydać użytkownikowi laptop zastępczy i przywrócić środowisko pracy.

5. Polityka bezpieczeństwa

Niniejsza polityka określa minimalne wymagania w zakresie ochrony urządzeń końcowych, nośników danych oraz dostępu fizycznego do infrastruktury teleinformatycznej. Obowiązuje wszystkich pracowników oraz współpracowników korzystających z zasobów organizacji.

5.1. Laptop pracownika

- Wszystkie laptopy są zaszyfrowane.
- Przy uruchamianiu systemu wymagany jest PIN, nadany przez użytkownika.
- Urządzenia wyposażone są w moduł TPM z ochroną przed atakami słownikowymi; w przypadku wykrycia takich prób system zażąda podania 48-cyfrowego klucza odzyskiwania.

5.2 Nośniki zewnętrzne (dyski, pendrivy itp.)

- Wszystkie zewnętrzne nośniki danych są dodatkowo szyfrowane z wykorzystaniem BitLocker.

5.3 Karty dostępu do budynku

- Każda karta dostępu posiada unikalny numer identyfikacyjny (ID) przypisany imiennie do pracownika w systemie kontroli dostępu.
- Z uwagi na autonomiczny charakter systemu, karty tymczasowe dla gości nie są wydawane..

5.4 Dostęp do serwerowni

- Pomieszczenie serwerowni jest trwale zabezpieczone; drzwi pozostają zamknięte
- Szafy serwerowe (rack) pozostają zamknięte i zabezpieczone.

Tomasz Kaźmierczak

Specjalista ds. Informatyki

6. Analiza ryzyka

Skala: niskie, średnie, wysokie.

6.1 Awaria serwera pocztowego

Ryzyko: niskie

Opis: Z uwagi na fakt że prowadzona jest Wojna na Ukrainie, Polskie firmy hostingowe są bardzo mocno narażone na różnego rodzaju niebezpieczeństwa. W przypadku całkowitej awarii serwera pocztowego, Spółka posiada zapasowy serwer pocztowy. Przełączenie poczty na zapasowy serwer pocztowy może trwać do 24 godzin z uwagi na odświeżenie usług DNS

6.2 Brak internetu - awaria głównego łącza oraz zapasowego

Ryzyko: niskie

Opis: Aktualnie jest bardzo dużo wykonywanych prac wokół Żeliwne 38, co niesie za sobą niskie ryzyko uszkodzenia przewodów światłowodowych które są doprowadzone do budynku. W przypadku całkowitego braku interetu, należy stworzyć lokalny hotspot i podłączyć pod 3 port w FortiGate 40E lub łączyć się bezpośrednio z laptopem.

6.3 Ransomware / Wirus

Ryzyko: niskie

Opis: Aktualnie wszystkie firmy w Polsce są narażone na różnego rodzaju ataki.W przypadku zaszyfrowania laptopa, ryzyko rozprzestrzenienia się na kolejne urządzenia jest niskie. W przypadku zaszyfrowania należy w całości wyczyścić komputer. Przeskanować kopie zapasową i w przypadku braku wykrycia odzyskać kopię zapasową.

Tomasz Kaźmierczak

Specjalista ds. Informatyki

Tomasz Kaźmierczak