



Pierwszy serwis IT, który mówi Twoim językiem



biuro@profinformatyka.pl



tel. 222 437 300



www.profinformatyka.pl

Dla właściciela firmy

Pomożemy Ci ogarnąć IT w Twojej firmie – bez technicznego żargonu i zbędnych stresów. Bo przecież masz lepsze rzeczy do roboty niż martwić się awariami komputera!

IT nie musi być czarną magią. W tym przewodniku pokażemy Ci, jak zarządzać wsparciem technicznym w firmie, jakie informacje zebrać i czego wymagać we współpracy z Panem (z reguły 😊) od informatyki.

Dlatego zebraliśmy najważniejsze zasady, które pomogą Ci kontrolować IT, zamiast gasić pożary co tydzień.



WSPARCIE
INFORMATYCZNE



STAŁA
OPIEKA IT



BEZPIECZEŃSTWO
DANYCH



DORADZTWO
TECHNICZNE



DEDYKOWANY
OPIEKUN

A. Najistotniejsze kwestie w obszarze obsługi

1

BEZPIECZEŃSTWO DANYCH I SYSTEMÓW

- Ochrona przed cyberatakami, ransomware, wyciekami danych
- Regularne aktualizacje, firewalle, szyfrowanie, kontrola dostępu
- Szkolenia pracowników z zakresu cyberbezpieczeństwa

2

CIĄGŁOŚĆ DZIAŁANIA (MINIMALIZACJA PRZESTOJÓW)

- Gwarancja wysokiej dostępności systemów (np. chmura, redundancja)
- Szybkie reagowanie na awarie (SLA – czas naprawy)
- Monitoring infrastruktury w czasie rzeczywistym

3

SKALOWALNOŚĆ I ELASTYCZNOŚĆ

- IT musi rosnąć wraz z firmą (np. rozbudowa serwerów, wdrożenie nowych narzędzi)
- Chmura, rozwiązania hybrydowe, automatyzacja procesów

4

KOSZTY I PRZEWIDYWALNOŚĆ BUDŻETU

- Model opłat dostosowany do potrzeb (np. abonament vs. pay-as-you-go)
- Unikanie ukrytych kosztów (np. nieplanowane naprawy)

5

WSPARCIE TECHNICZNE I DOSTĘPNOŚĆ

- Pomoc 24/7, zwłaszcza dla firm działających globalnie
- Jedno źródło wsparcia (np. outsourcing IT) zamiast rozproszenia





ZDALNE WSPARCIE

6

BACKUP I ODZYSKIWANIE DANYCH

- Regularne kopie zapasowe (również w chmurze)
- Plan Disaster Recovery (DRP) na wypadek katastrof (przywracanie infrastruktury i dostępu do danych)

7

ZGODNOŚĆ Z REGULACJAMI (COMPLIANCE)

- Dostosowanie do RODO, ISO, branżowych wymogów (np. fintech, medycyna)
- Audyty i dokumentacja procesów IT

8

WSPARCIE STRATEGICZNE

- Doradztwo w zakresie nowych technologii (AI, IoT, digital transformation)
- Optymalizacja narzędzi pod kątem konkurencyjności

9

INTEGRACJA SYSTEMÓW

- Spójność między narzędziami (np. CRM, ERP, komunikacja)
- Minimalizacja „siloś w informacyjnych”

10

PROAKTYWNOŚĆ

- Zapobieganie problemom (np. predictive maintenance)
- Regularne przeglądy infrastruktury i aktualizacje.

?

Dlaczego to ważne?

Awaria IT może sparaliżować ciągłość działania firmy, narazić na straty wizerunkowe lub/i finansowe. Jednocześnie dobrze zarządzane IT to szansa na optymalizację kosztów, innowacje i przewagę konkurencyjną.

B. Rozpoczęcie współpracy z nową firmą w zakresie wsparcia IT

Oto praktyczny plan działania, oparty na wcześniejszych wskazówkach:

1 DIAGNOZA POTRZEB I PRIORYTETÓW FIRMY

- **Audyt obecnej infrastruktury IT**
Zidentyfikuj słabe punkty (np. przestarzały sprzęt, brak backupu, luki w bezpieczeństwie)
- **Określ cele biznesowe**
Czy potrzebujesz wsparcia w migracji do chmury, wdrożeniu nowych systemów (CRM/ERP), czy głównie utrzymaniu istniejącej infrastruktury?
- **Zdefiniuj budżet**
Ustal, czy preferujesz model abonamentowy (stały koszt), czy płatność za usługi w miarę potrzeb (*pay-as-you-go*)

2 WYBÓR ODPOWIEDNIEGO PARTNERA IT

Stwórz krótką listę dostawców

- Szukaj firm z doświadczeniem w Twojej branży (np. fintech, e-commerce) i sprawdzonymi referencjami

Zweryfikuj zakres usług

- Czy oferują kompleksowe wsparcie (helpdesk, cyberbezpieczeństwo, backup, doradztwo)?

Sprawdź zgodność z compliance

- Upewnij się, że rozumieją wymagania prawne Twojej branży (np. RODO, ISO 27001).

3 WSTĘPNE KONSULTACJE I USTALENIE SLA

Spotkanie z dostawcą usług IT

- Opowiedz o swoich bolączkach i celach. Dobry partner zada szczegółowe pytania o procesy w Twojej firmie

Negocjuj SLA (Umowa o poziomie usług). Określ m.in.:

- Czas reakcji na zgłoszenia (np. 2 godziny dla krytycznych awarii)
- Dostępność wsparcia (24/7 czy tylko w godzinach pracy)
- Gwarancje dotyczące backupu i odzyskiwania danych (RTO/RPO)

IT dla Ciebie



WSPARCIE
INFORMATYCZNE

4

WDROŻENIE I INTEGRACJA

Stwórz harmonogram działań:

- Ustal etapy współpracy (np. migracja danych, szkolenia pracowników, wdrożenie monitoringu)

Wyznacz osoby kontaktowe:

- Po swojej stronie i u dostawcy – unikniesz chaosu w komunikacji.

Wdróż system raportowania:

- Regularne spotkania / raporty serwisowe (np. comiesięczne) - czas reakcji, liczba incydentów, postęp projektów

5

BEZPIECZNE ZARZĄDZANIE DOSTĘPEM I DANYMI

Przełącz niezbędne uprawnienia:

- Zastosuj zasadę ****najmniejszych przywilejów**** – dostawca IT powinien mieć dostęp tylko do tego, co konieczne

Podpisz NDA (umowę o poufności):

- Chroni Twoje dane i know-how

6

STAŁE DOSKONALENIE WSPÓŁPRACY

Regularne przeglądy usług (QBR – Quarterly Business Reviews):

- Omawiaj zmieniające się potrzeby firmy i nowe technologie

Wdrażaj rekomendacje dostawcy:

- Np. automatyzacja procesów, aktualizacja polityk bezpieczeństwa.

C. Kluczowe pytania, które warto zadać dostawcy przed

1. Jakie macie doświadczenie w mojej branży?
2. Czy macie certyfikaty (np. Microsoft Partner)?
3. Czy zapewniacie wsparcie zdalne i na miejscu?
4. Jak wygląda proces zgłaszania i eskalacji incydentów?
5. Czy macie przykładowe scenariusze Disaster Recovery dla firm mojej wielkości?

D. Czego unikać?

- Niejasnych umów – precyzyjnie definiuj zakres odpowiedzialności
- Dostawców bez elastyczności – IT musi skalować się z Twoim biznesem
- Ignorowania kultury współpracy – partner IT powinien rozumieć Twoje wartości i sposób pracy.



Podsumowanie

Najważniejsze to traktować współpracę z firmą IT jako partnerstwo, a nie transakcję. Dobre wsparcie technologiczne to nie tylko gaszenie pożarów, ale też strategiczny element rozwoju biznesu.



Osobiście Ci gwarantuję
– 100% satysfakcji lub zwrot pieniędzy.

Piotr Duchewicz

Checklista informacji, które firma IT powinna przejąć na etapie wdrożenia wsparcia

Pozwoli to uniknąć luk w wiedzy i zapewni płynne przejęcie usług:

1

INFORMACJE OGÓLNE O FIRMIE

Struktura organizacyjna: liczba pracowników, oddziały, kluczowe działy (np. finanse, HR, sprzedaż)

Godziny pracy firmy: czy wymagane jest wsparcie 24/7?

Kluczowe aplikacje biznesowe: np. system ERP, CRM, programy księgowe

Procesy biznesowe uzależnione od IT: np. sprzedaż online, magazyn, płatności

2

INFRASTRUKTURA IT

Lista serwerów (fizycznych/wirtualnych): specyfikacje, systemy operacyjne, role (np. plikowy, bazodanowy)

Urządzenia końcowe: liczba i typy komputerów, systemy operacyjne, urządzenia mobilne

Urządzenia sieciowe: modele routerów, switchy, firewalle, punkty dostępowe

Chmura: wykorzystywane usługi (Azure, AWS, Google Cloud), konta administratorów

3

SIEĆ I ŁĄCZNOŚĆ

Schemat sieci: topologia, adresacja IP, VLAN-y

Dostawcy internetu: SLA, przepustowość łącza

VPN: konfiguracja, protokoły, dostęp dla zdalnych pracowników

Kontrola ruchu sieciowego: reguły firewalli, polityki QoS

4

BEZPIECZEŃSTWO IT

Aktualne zagrożenia: znane luki w zabezpieczeniach lub incydenty (np. phishing, ransomware)

Narzędzia ochronne: antywirusy, EDR, SIEM, skanery podatności

Polityki bezpieczeństwa: zasady haseł, uwierzytelnianie wieloskładnikowe (MFA), kontrola dostępu

Historia incydentów: kiedy i jak reagowano na ataki/wycieki



PARTNERSTWO WSPÓŁPRACA - ZYSK

Dołącz do grona osób polecających
nasze rozwiązania i usługi.

Nasze **WSPARCIE IT** - zawsze pod ręką.



5

OPROGRAMOWANIE I LICENCJE

Wykaz licencji: systemy operacyjne, oprogramowanie biurowe, specjalistyczne narzędzia.

Klucze aktywacyjne i konta: dostęp do portali (np. Microsoft 365, Adobe).

Umowy maintenance: wsparcie producentów (np. SAP, Oracle).

6

BACKUP I ODZYSKIWANIE DANYCH

Strategia backupu: harmonogram, narzędzia (Veeam, Acronis), lokalizacje (dysk, chmura).

Parametry RTO/RPO: maksymalny dopuszczalny czas przestoju i utrata danych.

Procedura Disaster Recovery: dokumentacja odtwarzania systemów po awarii.

7

UŻYTKOWNICY I UPRAWNIENIA

Lista kont użytkowników: domeny, konta uprzywilejowane (admini).

Struktura Active Directory/LDAP: grupy, polityki, GPO.

Dostęp do krytycznych systemów: np. serwerów, baz danych.

8

DOKUMENTACJA I PROCESY

Dokumentacja techniczna: schematy sieci, konfiguracje urządzeń, hasła (w bezpiecznym repozytorium).

Procedury IT: np. onboardingu nowych pracowników, zgłaszania incydentów.

Umowy z dostawcami: np. serwisowymi, hostingowymi.

9

WYMAGANIA PRAWNE I COMPLIANCE

Obowiązujące regulacje: RODO, ISO 27001, branżowe standardy (np. PCI DSS dla płatności).

Raporty i audyty: wyniki ostatnich kontroli bezpieczeństwa.

Polityki prywatności: zasady przetwarzania danych klientów.

10 ISTNIEJĄCY DOSTAWCY IT

Kontakty do dostawców: np. serwisantów sprzętu, hostingu.

Umowy SLA: obowiązujące zobowiązania czasowe (np. gwarancja reakcji w 4h).

11 CELE BIZNESOWE I OCZEKIWANIA

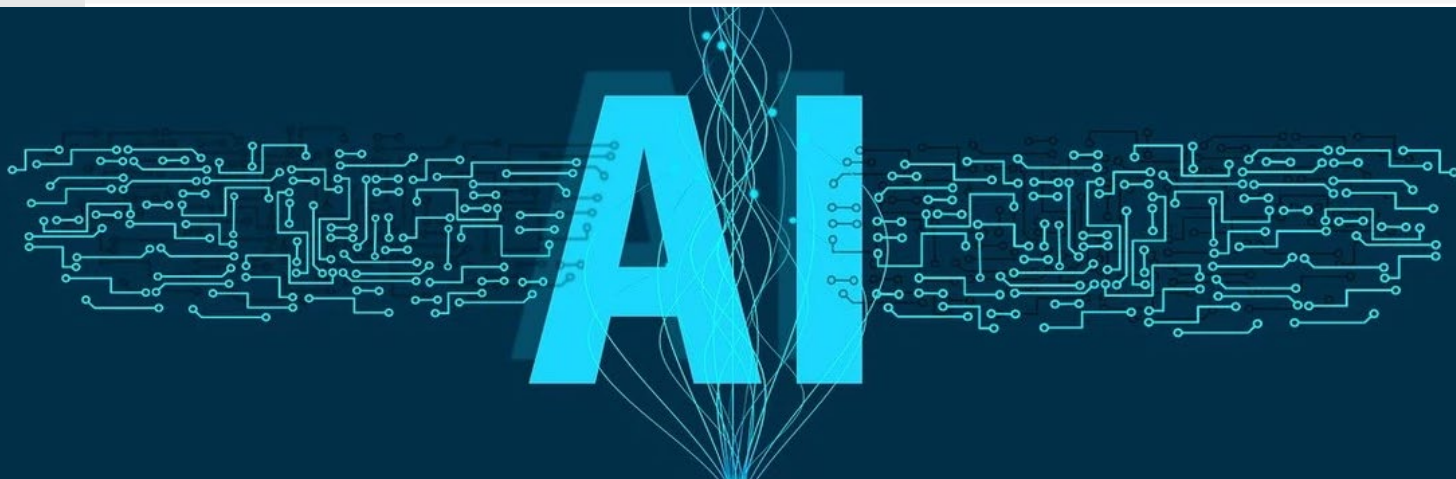
Krótko- i długoterminowe plany rozwoju: np. wdrożenie nowej filii, migracja do chmury.

Problemy do rozwiązania: np. wolne działanie systemów, brak monitoringu.

12 DOSTĘP I AUTORYZACJE

Dane dostępowe: konta administratorów, hasła do urządzeń, klucze SSH.

Kontakt do osoby decyzyjnej: kto zatwierdza zmiany w infrastrukturze?



Dodatkowe uwagi (dla Wsparcia IT)

- Weryfikacja danych: Przetestuj dostęp do wszystkich systemów przed podpisaniem umowy.
- Narzędzia do zarządzania: Upewnij się, czy klient używa np. RMM (Remote Monitoring and Management) lub innych platform.
- Szkolenia: Czy pracownicy potrzebują wprowadzenia do nowych procesów?



Dlaczego to ważne?

Kompletna dokumentacja minimalizuje ryzyko przestojów, konfliktów i luk w bezpieczeństwie. Im więcej szczegółów przekazesz dostawcy IT, tym sprawniej będzie mógł reagować na Twoje potrzeby!

Zestaw bardziej zaawansowanych informacji dla dociekliwych

Poniższe prace powinny być realizowane w ramach dobrze pojętej opieki informatycznej. Oczywiście zakres uzależniony jest w dużej mierze od tego jak rozbudowana jest infrastruktura informatyczna w Twojej firmie. Dlatego zakres prac i wykorzystanie narzędzi zależy już do oceny specjalisty.

Szczegółowe działania wspierające pro aktywność w zarządzaniu IT, które pozwalają uniknąć awarii i optymalizować infrastrukturę:

1 PREDICTIVE MAINTENANCE (PROAKTYWNA KONSERWACJA) MONITOROWANIE I ANALIZA DANYCH:

Wdrożenie systemów monitorowania w czasie rzeczywistym:

- Narzędzia: Nagios, Zabbix, PRTG, Datadog
- Metryki: wykorzystanie CPU/RAM, temperatura urządzeń, stan dysków (SMART), opóźnienia sieci.

Analiza predykcyjna z wykorzystaniem AI/ML:

- Wykrywanie wzorców prowadzących do awarii (np. rosnąca liczba błędów na dysku SSD)
- Narzędzia: Splunk ITSI, Azure AI, AWS Predictive Maintenance
- Alerty o anomaliach: Automatyczne powiadomienia o nietypowej aktywności (np. nagły wzrost ruchu sieciowego)

ZAPOBIEGANIE AWARIOM SPRZĘTU:

Regularne przeglądy fizyczne:

- Czyszczenie serwerów z kurzu, wymiana podzespołów (np. wentylatorów) przed ich awarią
- Kontrola zasilaczy UPS i warunków w serwerowni (temperatura, wilgotność)

Wymiana komponentów „przed upływem MTBF”:

- MTBF (Mean Time Between Failures) – np. wymiana dysków HDD po 3 latach eksploatacji

OPTIMALIZACJA OPROGRAMOWANIA:

Aktualizacje prewencyjne:

- Łatanie znanych luk w oprogramowaniu przed ich wykorzystaniem przez atakujących
- Automatyzacja aktualizacji przez narzędzia jak WSUS, Ansible, Puppet
- Usuwanie zbędnych usług: Wyłączanie nieużywanych portów, demonów lub aplikacji, które zwiększają powierzchnię ataku

2

REGULARNE PRZEGLĄDY INFRASTRUKTURY CYKL AUDYTÓW:

Przegląd sprzętu:

- Co 6 miesięcy: Sprawdzenie stanu fizycznego urządzeń (serwery, switchy, zasilacze)
- Testy obciążeniowe: Symulacja peak trafficu, aby wykryć słabe punkty

Audyt bezpieczeństwa:

- Co kwartał: Skanowanie podatności (Nessus, OpenVAS), przegląd logów pod kątem podejrzanych logowań
- Penetration testing: Raz w roku – testy przez zewnętrznych ekspertów

OPTYMALIZACJA ZASOBÓW:

Analiza wykorzystania chmury:

- Usuwanie nieużywanych maszyn wirtualnych, skalowanie w dół podczas okresów niższego ruchu
- Narzędzia: AWS Trusted Advisor, Azure Cost Management

Zarządzanie przechowywaniem danych:

- Archiwizacja starych danych, usuwanie duplikatów

3

AUTOMATYZACJA I STANDARYZACJA

Konfiguracja infrastruktury jako kod (IaC):

- Narzędzia: Terraform, Ansible – zapewnienie spójności środowisk (dev, test, prod)

Automatyczne skrypty:

- Resetowanie haseł, czyszczenie logów, zarządzanie kontami użytkowników

Polityka aktualizacji:

- Harmonogramy „Patch Tuesday” dla systemów Windows/Linux

4

SZKOLENIA I KULTURA PRO AKTYWNOŚCI

Warsztaty dla zespołu IT:

- Analiza root cause (RCA) po incydentach – jak uniknąć powtórzeń
- Symulacje reakcji na awarie (np. atak DDoS)

Programy zgłaszania inicjatyw:

- Nagradzanie pracowników za pomysły optymalizacji (np. redukcja kosztów chmury o 20%)

5

PLANOWANIE NA PODSTAWIE TRENDÓW

Analiza danych historycznych:

- Identyfikacja sezonowości (np. wzrost ruchu w e-commerce przed świętami).
- Przygotowanie infrastruktury na przewidywane obciążenia.

Benchmarking:

- Porównanie wydajności systemów z branżowymi standardami (np. czas odpowiedzi serwera).

6

WSPÓŁPRACA Z DOSTAWCAMI**Subskrypcje proaktywnego wsparcia:**

- Umowy z dostawcami sprzętu (np. Dell ProSupport) na wymianę części *zanim* ulegną awarii

Monitoring dostaw zewnętrznych:

- Śledzenie statusu usług kluczowych dostawców (np. hosting, CDN) poprzez integrację z ich API.

**Dlaczego to ważne?**

Pro aktywność w IT to nie tylko oszczędność kosztów, ale też „spokojna głowa” w codziennym działaniu i eliminacja stresu związanego z awariami. Dzięki wczesnemu wykrywaniu problemów firma może skupić się na rozwoju, zamiast gaszeniu pożarów.

Przykładowe działania wg harmonogramu

- Przegląd logów bezpieczeństwa – codziennie
- Testy obciążeniowe – co miesiąc
- Audyt podatności – co kwartał
- Szkolenia zespołu IT – co 6 miesięcy
- Wymiana dysków w serwerach – co 3 lata (wg MTBF)

KPI (Kluczowe wskaźniki skuteczności):

- MTBF (Mean Time Between Failures): Im wyższy, tym lepsza pro aktywność
- Liczba wykrytych incydentów zanim wpłynęły na biznes: Np. 95% awarii rozwiązanych przed wystąpieniem przestoju
- Procent zautomatyzowanych procesów: Cel: 80% rutynowych zadań.

**Czy potrzebujesz wsparcia w doborze narzędzi
lub wdrożeniu konkretnych procesów?**

Daj znać!

