WERYFIKACJA OGÓLNYCH KONTROLI IT

Ocena budowy i funkcjonowania kontroli IT w środowisku IT Spółki

I. ZARZĄDZANIE ŚRODOWISKIEM IT

1. Organizacja działu IT

1.1 Ile osób liczy dział IT i jaka część tych osób pełni funkcje administratorskie w systemach IT? Czy jest wyznaczony kierownik/dyrektor IT lub inna dedykowana osoba odpowiedzialna za obszar IT?

opisz sytuację
załącz strukturę organizacyjną – jeśli jest dostępna

W Spółce nie ma wydzielonego działu IT.
W Biurze Zarządu zatrudnionych jest dwóch pracowników – specjalistów w zakresie IT (Inspektor Ochrony Systemów i Sieci Teleinformatycznej. Inspektor Ochrony Danych oraz Specjalista ds. Informatyki). Służbowo podlegają Kierownikowi Biura Zarządu.

1.2 Czy pracownicy działu IT posiadają odpowiednią wiedzę i doświadczenie zgodne z zakresem ich obowiązków? Czy pracownicy mają możliwość odbywania okresowych szkoleń celem podnoszenia kwalifikacji?

TAK
Pracownicy mają możliwość podnoszenia kwalifikacji

2. Polityki i procedury

2.1 Czy istnieje formalna strategia/plan/koncepcja rozwoju środowiska IT?

załącz dokument
opisz istotne planowane zmiany dot. środowiska IT w Spółce

Tak, strategia rozwoju środowiska IT określona jest przez PGE S.A.
Spółka poprzez przyjęcie do stosowania „Kodeks Grupy PGE" wpisuje się w tą strategię w zakresie niezbędnym do realizacji celów biznesowych.

2.2. Czy istnieje formalna polityka bezpieczeństwa IT lub inny dokument określający wymagania związane z bezpiecznym korzystaniem z systemów i infrastruktury IT?

załącz dokument
Tak, dokument w załączeniu

II. BEZPIECZEŃSTWO FIZYCZNE

ograniczenie zakresu

*Ocena kontroli w obszarze Bezpieczeństwo fizyczne dotyczy wyłącznie systemów IT zidentyfikowanych w Spółce jako kluczowe (krytyczne) systemy IT – patrz dokument **511. Zrozumienie środowiska IT** – punkt **4.2***

ograniczenie zakresu

*Ocena kontroli w obszarze Bezpieczeństwo fizyczne dotyczy wyłącznie systemów IT, które funkcjonują na serwerach zlokalizowanych w pomieszczeniach (w serwerowni) Spółki, czyli nie zostały przekazane zewnętrznemu dostawcy – patrz dokument **511. Zrozumienie środowiska IT** – punkt **2.2***

3. Dostęp fizyczny

3.1 Czy serwery, na których zainstalowane są kluczowe systemy IT umieszczone są w dedykowanym, przeznaczonym do tego celu pomieszczeniu serwerowni, do którego dostęp jest odpowiednio chroniony, tj.:

- ✓ wejście jest zabezpieczone solidnymi drzwiami, które zamykane są na zamek i/lub kartę zbliżeniową
- ✓ nie ma możliwości dostępu przez okno, wewnętrzne drzwi z innego pomieszczenia, etc.

- ✓ dostęp do pomieszczenia jest monitorowany za pomocą kamer CCTV

Kluczowe systemy IT są udostępnione Spółce na podstawie zawartej umowy ze spółką PGE Systemy S.A. , która świadczy usługi ICT dla całej GK PGE. Zgodnie z zawartą umową PGE Systemy S.A. zapewnia odpowiednie zabezpieczenia fizyczne dla lokalizacji w których znajdują się serwery.
Pomocnicze systemy będące w posiadaniu Spółki umiejscowione są we własnej serwerowni zlokalizowanej w budynku Spółki do której dostęp wymaga przejścia przez bramę chroniona przez wykwalifikowana ochronę a teren jest objęty monitoringiem CCTV.
Pomieszczenie znajduje się za dwoma drzwiami zamykanymi na zamki patentowe a samo pomieszczenie serwerowni dodatkowo ma system antywłamaniowy.

3.2 Czy dostęp do pomieszczenia serwerowni posiadają jedynie wybrane, odpowiednio zatwierdzone osoby?

*Tak, dostęp do serwerowni posiadają wyłącznie upoważnieni pracownicy***.**

4. Bezpieczeństwo środowiska

4.1 Czy pomieszczenie serwerowni wyposażone jest w odpowiednie zabezpieczenia środowiskowe pod kątem ryzyka uszkodzenia serwerów ze względu na przegrzanie, pożar, zalanie, takie jak:

- ✓ klimatyzacja, zapewniającą odpowiednią temperaturę i wilgotność w pomieszczeniu,
- ✓ czujniki temperatury i wilgotności, na bieżąco monitorujące parametry środowiska, wraz z informowaniem o zmianach parametrów powyżej założonych progów
- ✓ system gaszenia gazem (wersja max), lub czujki dymu i gaśnice (wersja podstawowa)
- ✓ zabezpieczenie serwerowni i serwerów przed zalaniem, tj. serwery umieszczone w szafach powyżej poziomu podłogi (lub podłoga w serwerowni jest podniesiona), brak w pomieszczeniu rur z wodą, pomieszczenie nie jest bezpośrednio pod dachem
- ✓ system podtrzymania napięcia (UPS) i/lub dodatkowe źródło zasilania w razie awarii (np. niezależna linia zasilająca, generator)

zaplanuj wizytę w serwerowni i opisz poziom zabezpieczeń środowiskowych
Serwerownia w której znajdują się Kluczowe systemy IT zgodnie z zawartą umową ze spółką PGE Systemy S.A. zapewnia odpowiednie zabezpieczenia środowiskowe. Brak możliwości wizytacji serwerowni.

Serwerownia własna
możliwy termin wizyty – styczeń -luty 2026
wyposażenie środowiskowe:
klimatyzacja, czujki dymu i gaśnice, serwery umieszczone powyżej poziomu podłogi, brak w pomieszczeniu rur z wodą (za wyjątkiem C.O.), system podtrzymania napięcia (UPS) dla kluczowych urządzeń

III. BEZPIECZEŃSTWO LOGICZNE

ograniczenie zakresu
Ocena kontroli w obszarze Bezpieczeństwo logiczne dotyczy wyłącznie systemów IT zidentyfikowanych w Spółce jako kluczowe (krytyczne) systemy IT – patrz dokument ***511. Zrozumienie środowiska IT*** *– punkt* ***4.2***

5. Zarządzanie użytkownikami

5.1 Czy istnieje formalna procedura/instrukcja, lub usystematyzowany proces dotyczące zarządzania użytkownikami systemów IT, obejmujące następujące elementy:

- ✓ proces wnioskowania i zatwierdzania założenia nowych użytkowników przez przełożonych/osoby upoważnione z użyciem np. dedykowanego narzędzia IT/ zatwierdzeń mailowych
- ✓ określenie zakresu uprawnień użytkowników w systemach na podstawie zakresu ich zadań oraz zatwierdzenie uprawnień przez przełożonych/osoby upoważnione
- ✓ efektywny proces blokowania dostępu do systemów dla użytkowników w razie potrzeby (np. z powodu rozwiązania umowy o pracę)

załącz procedurę/instrukcję dotyczącą zarządzania użytkownikami
opisz proces
Procedura w załączeniu

5.2 Czy są wykonywane okresowe przeglądy aktywnych użytkowników i ich uprawnień w systemach IT w celu potwierdzenia, że tylko upoważnione osoby mają dostęp do systemów, a zakres ich uprawnień jest zgodny z zakresem obowiązków?

załącz dokumentację z przeglądu użytkowników
arkusz z weryfikacji uprawnień w załączeniu

5.3 Czy została przeprowadzona analiza uprawnień użytkowników pod kątem ewentualnych konfliktujących uprawnień (Segregation of Duties - SOD)? Czy w Spółce przygotowano macierz konfliktujących uprawnień?

załącz dokumentację z przeglądu SOD
załącz matrycę konfliktujących uprawnień w organizacji
SOD przeprowadza PGE Systemy S.A.
Matryca konfliktów w załączeniu

6. Dostępy uprzywilejowane

6.1 Czy istnieje formalna, zatwierdzona przez upoważnione osoby, lista osób które posiadają uprzywilejowany (administratorski) dostęp do systemów IT, w tym na poziomie aplikacji, systemu operacyjnego i bazy danych?

Nie dotyczy
Spółka nie posiada administratorskiego dostępu do kluczowych systemów IT. Całość zarządzana jest przez PGE Systemy w oparciu o podpisana umowę.

6.2 Czy występuje zastępowalność w przypadku niedostępności kluczowych administratorów?

Nie dotyczy

6.3 Czy inni użytkownicy, poza administratorami systemów IT, mają bezpośredni dostęp (z pominięciem aplikacji) na poziomie systemu operacyjnego (OS) lub bazy danych (DB)?

Nie dotyczy

6.4 Czy w Spółce istnieją narzędzia pozwalające na monitorowanie aktywności na kontach uprzywilejowanych, w tym historii logowania się na konta administratorskie oraz rejestracji czynności wykonywanych za ich pomocą?

zweryfikuj istnienie narzędzi monitorujących
opisz proces
załącz prnt scrn z narzędzi monitorujących
Nie dotyczy

7. Restrykcje logowania

7.1 Czy wszyscy użytkownicy kluczowych systemów IT korzystają z indywidualnych, przypisanych tylko do nich kont w systemach?

opisz proces
Tak

7.2 Czy konta użytkowników chronione są unikalnymi hasłami, które spełniają minimalne wymagania, takie jak:

- ✓ określona minimalna dł. hasła
- ✓ wymagania dot. okresowej zmiany hasła
- ✓ monitorowanie historii haseł
- ✓ blokowanie konta po nieudanych próbach zalogowania

- ✓ aktywny wygaszacz ekranu (screen saver) automatycznie blokujący dostęp do stacji roboczej

opisz proces logowania *załącz prnt scrn z restrykcjami logowania na poziomie systemu sieciowego (domena/Active Directory)* *załącz prnt scrn z restrykcjami logowania dla kluczowych systemów IT* *Dostęp do komputera, zasobów sieciowych Spółki oraz kluczowych systemów IT jest możliwy jedynie dla uwierzytelnionych Użytkowników. Uwierzytelnienie oparte jest o Konta Użytkowników pochodzące z Korporacyjnego Active Directory.* *Brak możliwości załączenia prt scr z restrykcjami logowania na poziomie systemu sieciowego oraz dla kluczowych systemów IT. Domena AD w której znajdują się komputery Spółki zarządzana jest przez pracowników PGE GiEK S.A o/Elektrownia Turów / PGE Systemy na mocy zawartej umowy na świadczenie usług.*

8. Zdalny dostęp

8.1 Czy pracownicy, klienci lub dostawcy posiadają zdalny dostęp do kluczowych systemów IT (np. przez VPN)? Jeśli tak, jakie zastosowano metody autoryzacji i monitorowania zdalnego dostępu?

opisz proces *załącz listę osób posiadających zdalny dostęp – w załączeniu* *załącz prnt scrn z narzędzi monitorujących* *Zasady dostępu do kluczowych zasobów opisane są w załączonym dokumencie* *Brak możliwości załączenia prt scr z narzędzi monitorujących.* *Domena AD w której znajdują się komputery Spółki oraz konta dostępowe do kluczowych systemów IT zarządzana jest przez pracowników PGE GiEK S.A o/Elektrownia Turów / PGE Systemy na mocy zawartej umowy na świadczenie usług.*

IV. UTRZYMANIE SYSTEMÓW

9. Aktualizacje i poprawki bezpieczeństwa

9.1 Czy wszystkie systemy IT i urządzenia, w tym stacje robocze, serwery, urządzenia sieciowe, etc. są aktualizowane na bieżąco, zgodnie z wymaganiami producenta/dostawcy?

opisz proces *załącz rejestr/dokumentację wdrażanych aktualizacji i poprawek* przykładowy raport w załączeniu

10. Ochrona antywirusowa

10.1 Czy system antywirusowy (AV) jest zainstalowany na wszystkich stacjach roboczych i serwerach Spółki? Czy system AV podlega regularnej aktualizacji?

opisz proces *załącz prnt scrn ze statusem AV dla stacji roboczej i kluczowych serwerów* przykładowy raport w załączeniu

11. Zarządzanie incydentami

11.1 Czy w Spółce funkcjonuje efektywny proces zarządzania incydentami, w ramach którego wszelkie błędy, problemy i nieprawidłowości w systemach IT są zgłaszane, rejestrowane i rozwiązywane?

opisz proces *załącz prnt scrn z narzędzia rejestrującego* Tak, proces zarządzany jest przez PGE Systemy oraz zespół CERT Spółka nie posiada dostępu do narzędzi rejestrujących. Spółka jest informowana o przypadkach incydentów jeżeli dotyczy to jej komputerów. Regulacje w załączeniu.

12. Zarządzanie siecią

12.1 Czy w Spółce funkcjonuje wydzielona sieć lokalna (LAN) łącząca komputery, serwery i inne urządzenia, umożliwiającą korzystanie ze współdzielonych zasobów, tj. systemów IT, plików, drukarek, etc.?

opisz topologię sieci oraz zakres współdzielonych zasobów udostępnianych w sieci LAN
załącz ogólny schemat sieci
Spółka nie posiada własnej infrastruktury sieciowej.
Dostęp do zasobów sieciowy realizowany jest po LAN na podstawie zawartych umów z PGE GiEK S.A. o Elektrownia Turów oraz z PGE Systemy S.A

12.2 W jaki sposób chroniona jest komunikacja między siecią LAN, a Internetem? Czy w ramach systemu zabezpieczeń przez zagrożeniami z zewnątrz organizacja korzysta z zapór sieciowych (firewall), serwerów proxy, stref DMZ, podsieci VLAN, systemów detekcji włamań, narzędzi monitorujących, etc.

opisz system zabezpieczeń chroniący przed zagrożeniami z zewnątrz
Spółka nie posiada własnej infrastruktury sieciowej.
Dostęp do sieci rozległej realizowany jest na podstawie zawartych umów z PGE GiEK S.A. o Elektrownia Turów oraz z PGE Systemy S.A

12.3 Czy w Spółce są wyznaczone osoby odpowiadające za administrację siecią lokalną (LAN) oraz systemem zabezpieczeń połączenia z Internetem? Czy osoby te monitorują na bieżąco funkcjonowanie urządzeń sieciowych oraz śledzą występujące incydenty i zdarzenia nie pożądane?

opisz zakres odpowiedzialności
opisz proces monitorowania
Spółka nie posiada własnej infrastruktury sieciowej.
Administracją i monitorowaniem sieci LAN zajmują się pracownicy PGE Systemy S.A

V. CIĄGŁOŚĆ DZIAŁANIA

ograniczenie zakresu

*Ocena kontroli w obszarze Ciągłości działania dotyczy wyłącznie systemów IT zidentyfikowanych w Spółce jako kluczowe (krytyczne) – patrz dokument **511. Zrozumienie środowiska IT** – punkt **4.2***

13. Kopie zapasowe (backup)

13.1 Czy Spółka wykonuje regularne kopie zapasowe (backup) kluczowych systemów IT? W jaki sposób, z użyciem jakich narzędzi, nośników i z jaką częstotliwością wykonywane są kopie zapasowe?

Czy istnieją formalne procedury/instrukcje/zasady opisujące sposób wykonywania kopii zapasowych, ich zakres oraz częstotliwość?

opisz sposób wykonywania kopii zapasowych, ich zakres, częstotliwość i używane narzędzia
załącz istniejące procedury/instrukcje/zasady wykonywania kopii bezpieczeństwa
załącz prnt scrn z narzędzia backupowego potwierdzający wykonanie backupu miesięcznego/rocznego

Backup z Kluczowych systemów realizowany jest przez spółkę PGE Systemy na mocy podpisanych umów. Brak możliwości przedstawienia prnt scr.
Backup z zasobów własnych Spółki realizowany jest automatycznie w cyklach dziennych i tygodniowych na urządzeniach dedykowanych. Przykładowe prt scr w załączeniu.

13.2 W jakiej lokalizacji i w jaki sposób przechowywane są kopie zapasowe?

opisz gdzie i w jaki sposób przechowywane są kopie zapasowe
w miarę możliwości zweryfikuj bezpieczeństwo fizyczne i zabezpieczenia środowiskowe w miejscu przechowywania

Z uwagi na fakt, że backup z Kluczowych systemów realizowany jest przez spółkę PGE Systemy na mocy podpisanych umów Spółka nie posiada wiedzy co do lokalizacji i sposobu przechowywania kopii zapasowych
Kopie zapasowe z zasobów własnych Spółki przechowywane są na dedykowanych urządzeniach w serwerowni do której dostęp jest ograniczony wyłącznie do osób wyznaczonych.

13.3 Czy kopie zapasowe są okresowo testowane pod kątem możliwości ich odtworzenia?

załącz protokoły/notatki/maile potwierdzające przeprowadzenie testów odtworzenia kopii zapasowych

tak, kopie są okresowo testowane w zakresie integralności i możliwości odtworzenia.
Przykładowy prt. Scr w załączeniu

13.4 Czy przygotowywane są okresowo tzw. 'zimne' kopie zapasowe, tj. niepodłączone do sieci/internetu w celu ochrony przed zewnętrznym atakiem typu 'ransomware', mogącym spowodować zaszyfrowanie danych w systemach IT?

opisz proces
tak, kopia taka jest realizowana na urządzeniu do którego nie mają dostępu uzytkownicy. Całość kopi przeprowadzana jest w sposób automatyczny. Urządzenie końcowe nie jest wystawione do sieci Internet.

14. Plany BCP/DRP

14.1 Czy powstały plany odtworzenia działalności w razie rozległej awarii (Disaster Recovery Plan - DRP) i/lub plany kontynuowania działalności (Business Continuity Plan - BCP) w celu zapewnienia, że krytyczne procesy biznesowe mogą być kontynuowane lub zostaną wznowione bez zbędnej zwłoki w przypadku wystąpienia nieprzewidzianych zdarzeń?

opisz sytuację
załącz kopie formalnie zatwierdzonych/wdrożonych dokumentów BCP i DRP

tak, w Spólce jest „Plan zapewnienia ciągłości działania w przypadku zakłócenia teleinformatycznego środowiska pracy"
dokument w załączeniu

14.2 Czy Spółka dysponuje zapasową infrastrukturą IT na wypadek wystąpienia rozległej awarii? Infrastruktura taka może obejmować np. zapasową serwerownię, kluczowe urządzenia, niezależne łącze sieciowe, zasilanie z alternatywnego źródła, etc.

opisz sytuację
Tak, Spółka dysponuje zapasowym łączem z dostepem do Internetu.

VI. ZARZĄDZANIE ZMIANĄ

ograniczenie zakresu

*Ocena kontroli w obszarze Zarządzania zmianą dotyczy wyłącznie systemów IT zidentyfikowanych w Spółce jako kluczowe (krytyczne) – patrz dokument **511. Zrozumienie środowiska IT** – punkt **4.2***

ograniczenie zakresu

*Ocena kontroli w obszarze Zarządzania zmianą dotyczy wyłącznie systemów IT typu MOTS oraz rozbudowanych systemów ERP, dla których występują zmiany funkcjonalne wnioskowane i wprowadzane przez użytkowników – patrz dokument **511. Zrozumienie środowiska IT** – punkt **4.3b** i **4.3c***

*Zarządzanie zmianą nie będzie miało również prawdopodobnie zastosowania dla systemów funkcjonujących w modelu oprogramowania jako usługi (Saas), gdzie możliwości modyfikacji i zmian są ograniczone w porównaniu z tradycyjnym oprogramowaniem (ale wymaga to potwierdzenia ze Spółką) – patrz dokument **511. Zrozumienie środowiska IT** – punkt **4.4***

15. Zarządzanie zmianą

15.1 Czy istnieją formalne procedury/instrukcje/zasady dotyczące zarządzania zmianami w systemach IT?

opisz sytuację
załącz kopię procedury/instrukcje/zasad dotyczących zarządzania zmianami

Procedura w załączeniu

15.2 Czy istnieją dedykowane narzędzia, w których zmiany są zgłaszane, rejestrowane, zatwierdzane, etc.?

opisz narzędzia wspierające zarządzanie zmianami

proces zarządzania zmianą dla kluczowych systemów IT nadzorowany jest przez PGE Systemy, które posiadają dedykowane narzędzia.

15.3 Czy istnieje podział na środowisko testowe, w którym zmiany są testowane przed ich uruchomieniem oraz docelowe środowisko produkcyjne, z którego na co dzień korzystają użytkownicy systemu?

opisz sytuację
załącz prnt scrn potwierdzający istnienie wydzielonego środowiska testowego

tak, środowisko testowe jest odseparowane od produkcyjnego. Zrzut w załączeniu, kolorem żółtym oznaczono dostęp do środowiska testowego dla kluczowych systemów

15.4 Czy występuje właściwy podział obowiązków (SOD) w obszarze rozwoju systemów zapewniający, że osoby przygotowujące zmiany do systemów nie posiadają dostępu i nie wykonują czynności w środowisku produkcyjnym?

opisz sytuację
zweryfikuj listę osób posiadających dostęp do środowiska produkcyjnego pod kątem występowania developerów/programistów
W zakresie użytkowników Spółki nie występują developerzy/programiści

VII. NARZĘDZIA EUC

ograniczenie zakresu

*Ocena kontroli w obszarze Narzędzia EUC dotyczy wyłącznie sytuacji, kiedy pracownicy Spółki dla celów procesowania i raportowania danych, poza kluczowymi systemami IT, wykorzystują dodatkowe narzędzia IT, takie jak arkusze kalkulacyjne, bazy danych Access i zapytania SQL – patrz dokument **511. Zrozumienie środowiska IT** – punkt **5. Dodatkowe narzędzia IT***

16. Ewidencja narzędzi EUC

16.1 Czy w organizacji istnieje rejestr/spis narzędzi EUC wykorzystywanych przez użytkowników dla celów procesowania i raportowania danych?

Biuro EK sposób skatalogowany umiejscawia raporty pod konkretne potrzeby raportowania (wewnętrzne i zewnętrzne). W łatwy sposób jest możliwe wskazanie konkretnego raportu. Brak listy – jako dokumentu z wypisanymi „z nazwy" wszystkimi raportami przygotowywanymi przez Biuro EK.

16.2 Czy istnieją kontrole obejmujące narzędzia EUC, zapewniające prawidłowość i kompletność procesowanych przez nie danych? Kontrole takie mogą obejmować przypisanie własności, kontrolę nad formułami, okresowe testowanie, automatyczne walidacje itp.

Biuro EK jako odpowiedzialny za wszelkie tworzone przez siebie raporty kontrolingowe z wykorzystaniem arkusza kalkulacyjnego sprawuje nadzór w sposób bieżący/ ciągły nad poprawnością danych.
Raportujemy do Centrali GiEK dane w arkuszach kalkulacyjnych, które w kolejnym etapie podlegają weryfikacji i walidacji danych ze wszystkich Spółek.
Do raportowania comiesięcznego oraz na potrzeby procesu planistycznego wykorzystywana jest również platforma internetowa SAP FC https://sapfc.gkpge.pl/FcWeb/login?NoSso=true , która służy do konsolidacji danych na potrzeby całej Grupy PGE.

VIII. ZEWNĘTRZNI DOSTAWCY (Service Organization)

ograniczenie zakresu

*Ocena kontroli w obszarze Zewnętrzni dostawcy dotyczy infrastruktury technicznej IT (serwery, urządzenia sieciowe, etc.) oraz systemów IT zidentyfikowanych w Spółce jako kluczowe (krytyczne) – patrz dokument **511. Zrozumienie środowiska IT** – punkt **4.2***

ograniczenie zakresu

Ocena kontroli w obszarze Zewnętrzni dostawcy dotyczy wyłącznie sytuacji, kiedy Spółka przekazała odpowiedzialność za utrzymanie środowiska IT lub jego części, w tym kluczowych systemów IT do zewnętrznych dostawców – patrz dokument ***511. Zrozumienie środowiska IT*** *– punkt* ***2.2***

17. Outsourcing IT

17.1 W jakim zakresie Spółka korzysta usług z dostawców zewnętrznych dla celów utrzymania i administracji środowiskiem IT?

opisz udział dostawców zewnętrznych w utrzymaniu i administracji środowiskiem IT
PGE Systemy S.A.:
Wsparcie procesów zarządzania przedsiębiorstwem w zakresie:
Wsparcie procesów biznesowych w obszarze rachunkowości i logistyki
Zarządzanie Kapitałem Ludzkim
Obieg Faktur Zakupowych w SAP
SAP AM (SAP Zarządzanie Majątkiem)
Komputerowe stanowisko pracy w zakresie:
Centralna domena (AD
Dostęp do sieci rozległej GK PGE
Zdalny dostęp
Platforma e-Learning
Dostawa i wsparcie aplikacji prawnych (LEX/Legalis)
Usługi telekomunikacyjne stacjonarne
Komunikator Osobisty
Wideokonferencje przez Wideoterminale

PGE GiEK S.A o/Elektrownia Turów:
Udostępnianie zasobów Internetowych – dostęp do sieci rozległej
Rozbudowa sieci LAN
Zarządzanie domeną

17.2 Czy istnieje formalna umowa określająca szczegółowo zakres świadczonych przez dostawcę usług, w tym kluczowe parametry usługi oraz definiująca podział odpowiedzialności pomiędzy stronami?

załącz kopię umowy opisującej usługi świadczone przez dostawcę
zweryfikuj, czy umowa określa kluczowe parametry usługi oraz definiuje zakresy odpowiedzialności

w załączeniu
umowa określa zarówno parametry jak i odpowiedzialność

Adam Kurzątkowski

Podpis cyfrowy: Adam Kurzątkowski
Data: 2025.12.08 08:42:56+01'00'