Park Naukowo-Technologiczny
w Opolu Sp. z o.o.
im. prof. Marka Tukiendorfa

PNT DATA CENTER

Wyciąg z polityki bezpieczeństwa PNT Data Center

PNT Data Center w Opolu to bezpieczne datacenter z certyfikatem ANSI/TIA 942 – RATED 3 którego działalność prowadzona jest z zachowaniem norm ISO9001 oraz ISO27001.

Bezpieczeństwo w systemach teleinformatycznych oraz ciągłość dostępności usług zapewnia się przez wdrożenie spójnego zbioru zabezpieczeń w celu zapewnienia poufności, integralności i dostępności informacji.

Cel o którym mowa osiąga się przez:

1. Utrzymywanie wysokiego poziom odporności na awarie infrastruktury Data Center dzięki spełnieniu określonych wymagań dotyczących redundancji i niezawodności w zakresie infrastruktury krytycznej według normy ANSI/TIA 942 – RATED 3.
2. Objęcie systemu teleinformatycznego politykami bezpieczeństwa oraz procesem zarządzania ryzykiem zgodnie z ISO27001.
3. Ograniczenie zaufania, polegające na traktowaniu innych systemów teleinformatycznych jako potencjalnych źródeł zagrożeń oraz wdrożeniu w systemie teleinformatycznym zabezpieczeń kontrolujących wymianę informacji z tymi systemami teleinformatycznymi.
4. Wprowadzenie wielopoziomowej ochrony systemu teleinformatycznego, polegającej na stosowaniu zabezpieczeń na możliwie wielu różnych poziomach organizacji ochrony systemu teleinformatycznego, w celu ograniczenia występowania przypadków, w których przełamanie pojedynczego zabezpieczenia skutkuje naruszeniem celu.
5. Wykonywanie okresowych testów bezpieczeństwa oraz auditów wewnętrznych zgodnie z procedurą „*Audity wewnętrzne*".

6. Ograniczanie uprawnień, polegające na nadawaniu użytkownikom systemu teleinformatycznego wyłącznie uprawnień niezbędnych do wykonywania pracy zgodnie z *„Polityka monitorowania systemu"*.
7. Monitorowanie oprogramowania, urządzeń oraz usług zgodnie z *„Polityka monitorowania systemu"*
8. Ograniczenie fizycznego dostępu do pomieszczeń i urządzeń centrum danych wyłącznie do upoważnionych pracowników posiadający właściwe uprawnienia i umiejętności.
9. Fizyczny dostęp do pomieszczeń i urządzeń centrum danych osób trzecich, będących klientami możliwy jest jedynie w asyście operatorów Data Center i jest monitorowany.
10. W celu zapewnienia dostępności zasobów w systemie teleinformatycznym ustala się:
    a. zasady tworzenia i przechowywania kopii zapasowych – *„Polityka kopii zapasowych"*;
    b. procedury postępowania w sytuacjach kryzysowych, w tym w przypadkach awarii elementów systemu teleinformatycznego;
    c. polityki aktualizacji oprogramowania na serwerach – *„Polityka zarządzania oprogramowaniem"*
    d. procedury monitorowania stanu technicznego systemu teleinformatycznego – *„Polityka monitorowania systemu"*.
11. W przypadku organizacji połączenia międzysystemowego organizując połączenie międzysystemowe, wdraża się zabezpieczenia uniemożliwiające przekazywanie niepożądanych informacji pomiędzy łączonymi systemami

teleinformatycznymi, w szczególności uniemożliwiające przekazywanie informacji o wyższej klauzuli tajności do systemu teleinformatycznego przetwarzającego informacje o klauzuli niższej.

12. W celu ochrony osób fizycznych w związku z przetwarzaniem danych osobowych stosuje się dodatkowo polityki zawarte w *„Regulamin Ochrony Danych Osobowych"*

Spis funkcjonujących polityk, na których oparte jest bezpieczeństwo informacji:

- PO/05 – Wymagania bezpieczeństwa systemów informacyjnych
- PO/06 – Polityka używania kluczy kryptograficznych
- PO/09 – Polityka kopii zapasowych
- PO/10 – Polityka postępowania ze sprzętem IT
- PO/11 – Polityka synchronizacji czasu
- PO/12 – Obsługa nośników wymiennych
- PO/13– Polityka haseł
- PO/14 – Polityka zarządzania oprogramowaniem
- PO/15 – Polityka zarządzania incydentami
- PO/16 – Polityka monitorowania systemu
- PO/17 – Polityka zasad postępowania w systemach
- PO/18 – Polityka zarządzania urządzeniami sieciowymi
- PO/19 – Wymagania bezpieczeństwa fizycznego urządzeń sieci
- PO/20 – Zarządzanie prawami dostępu do urządzeń sieciowych
- PO/21 – Segmentacja sieci
- PO/22 – Polityka monitorowania urządzeń sieciowych
- PO/23 – Polityka Synchronizacji zegara
- PO/24 – Polityka aktualizacji firmware w urządzeniach sieciowych
- PO/25 – Polityka kopii zapasowych konfiguracji urządzeń sieciowych
- PO/26 – Wdrażanie nowego urządzenia sieciowego
- PO/27 – Polityka przyjmowania i wydawania sprzętu sieciowego z Data Center
- PO/28 – Zdalny dostęp do zasobów
- PO/29 – Polityka dostępu do Data Center

- PO/30 – Polityka postępowania w przypadku alarmu pożarowego w DC
- PO/31 – Polityka przyznawania i odbierania karty dostępu
- PO/32 – Polityka usługi zdalnych rąk
- PO/33 – Polityka przyjmowania i wydawania sprzętu z Data Center

CERTYFIKACJA ANSI/TIA 942 – RATED 3

Certyfikat ANSI/TIA Rated 3 jest jednym z standardów określających poziom odporności na awarie infrastruktury. Data Center z certyfikatem Rated 3 cechują się wyższą niezawodnością, muszą one spełniać określone wymagania dotyczące redundancji i niezawodności w zakresie infrastruktury krytycznej.

Zabezpieczenia PNT Data Center:

Zasilanie

- Dwie niezależne linie energetyczne
- Dwa niezależne transformatory każdy o mocy 630 kW
- System UPS w redundancji 2N z podtrzymaniem na 10 min. mocy docelowej 400 kW
- Zasilanie szaf z niezawodnością 2N z zastosowaniem agregatu prądotwórczego (zasilanego paliwem płynnym) wraz z infrastrukturą umożliwiającą bezprzerwowe przełączenie zasilania
- Standardowy przydział mocy na szafę – 4,4 kW, docelowy po konsultacji z klientem

System gaszenia

- Powierzchnia kolokacyjna Centrum Przetwarzania Danych stanowi wydzieloną, niezależną strefę pożarową o odporności ogniowej ścian minimum 120 min

- Pomieszczenia wyposażone w czujniki dymu i temperatury oraz system VESDA
- Pomieszczenia wyposażone w zautomatyzowany, wielostrefowy system gaszenia na bazie mieszaniny gazów naturalnych – Inergen
- Pomieszczenia wyposażone w system wczesnego wykrywania dymu
- Wszystkie systemy ochrony przeciwpożarowej data center połączone z centralnym systemem zarządzania budynkiem.

Warunki klimatyczne

- Data center wyposażone jest w klimatyzację precyzyjną wraz z kontrolą i regulacją temperatury i wilgotności środowiska w układzie
- W/w system klimatyzacji pracujący w redundancji, w układzie N+1
- Utrzymywanie parametrów środowiskowych – temperatura 21 – 24 ° Celsjusza
- Utrzymywanie parametrów środowiskowych – wilgotność 20 – 60 %
- Kontrola i rejestracja parametrów środowiskowych z częstotliwością nie mniejszą niż 10 minut.
- System wykrywania wody na powierzchni kolokacyjnej Centrum Przetwarzania Danych

SYSTEM OCHRONY ANTY DDoS

- Ochrona anty DDoS Distributed Denial of Service zabezpiecza przed atakami wolumetrycznymi i zapewnia nieprzerwany dostęp klientów i użytkowników wewnętrznych do udostępnionych zasobów takich jak strony www, aplikacje, bazy danych i urządzenia sieciowe. W ramach usługi dostępu do Internetu w Data Center Opole, analizowany jest ruch sieciowy, monitorowany poziom wykorzystania łącza oraz prowadzona detekcja anomalii sieciowych.

Park Naukowo-Technologiczny
w Opolu Sp. z o.o.
im. prof. Marka Tukiendorfa

PNT DATA CENTER

Aktualny Certyfikat Centrum Przetwarzania Danych PNT w Opolu. Weryfikacja możliwa na stronie : https://www.epi-certification.com/sites/list/Poland/0/0

epi
Protecting your interests

CERTIFICATE OF CONFORMANCE
CONSTRUCTED FACILITY

This is to certify that the constructed data center facilities of

Park Naukowo-Technologiczny w Opolu Sp. z o.o.

ul. Technologiczna 2 Ground Floor - Parter PL45839
Opole, Poland

has been independently assessed and found to conform to the requirements of:

ANSI/TIA-942-B-2017

Rated-3

for the following scope:

Architecture	Telecom	Electrical	Mechanical
Rated-3	Rated-3	Rated-3	Rated-3

Certificate Number: TIA942PL220622001
Certificate validity: 22-Jun-2022 until 21-Jun-2025

Certification Manager
EPI Certification Pte Ltd

TIA-942 SM

Surveillance audits due by: June 2023 June 2024

Lack of fulfillment of certification terms and conditions may render this certificate invalid. This certificate can be verified at https://tiaonline.org/942-datacenters/

Wytyczne współpracy dyżurnego inżyniera z klientem i podwykonawcą

1. Zakres stosowania: Klienci i Podwykonawcy DATA CENTER
2. Zasady dostępu fizycznego

2.1 Na teren DATA CENTER, klienci lub podwykonawcy mogą wejść na podstawie dowodu tożsamości ze zdjęciem lub wydanego identyfikatora, po uzyskaniu autoryzacji jednorazowej wykonanej przez Dyżurnego Inżyniera lub autoryzacji poprzez Listę Dostępu.

2.2 W trakcie pierwszego wykonywania prac w DC, Klienci i Podwykonawcy:

2.2.1 Zapoznają się z podstawowymi informacjami o Data Center oraz dokumentami instruktażowymi.

2.2.2 Zostają przeszkoleni przez Dyżurnego Inżyniera o zasadach: poruszania się po obiekcie, bezpiecznego korzystania z DC, poufności informacji.

2.2.3 Podpisują odpowiednie oświadczenia o zapoznaniu się z zasadami obowiązującymi w DC oraz zobowiązujących ich do zachowaniu poufności.

2.3 W uzasadnionych przypadkach, Klient lub Podwykonawca może wystąpić o wydanie identyfikatora oraz karty dostępu umożliwiających poruszanie się na terenie obiektu w ramach przydzielonych uprawnień.

Autoryzacja

Wszystkie prace i dostawy zgłoszone do realizacji w DC podlegają autoryzacji.

Autoryzacja polega na weryfikacji przez Dyżurnego Inżyniera danych zgłoszonych formularzem: Lista Osób Upoważnionych do kontaktów i autoryzacji – uprawnień osób zgłaszających się do wykonania prac lub dostawy.

Jeśli zgłaszający się nie posiada odpowiednich uprawnień, Dyżurny Inżynier nie wyrazi zgody na wykonanie prac na terenie DC lub przyjęcie dostawy. W uzasadnionych lub wyjątkowych sytuacjach Dyżurny Inżynier wykonuje dodatkowo autoryzację prac lub dostaw z jedną z osób uprawnionych do autoryzacji w formularzu Lista Osób Upoważnionych do kontaktów i autoryzacji. Zmiana listy osób upoważnionych może nastąpić jedynie poprzez przekazanie do DATA CENTER zmodyfikowanej, oryginalnej listy w formie pisemnej – koniecznie zatwierdzonej i podpisanej przez klienta lub zostanie zaktualizowana mailowo z adresu wskazanego w umowie jako dane kontaktowe do współpracy.

3. Zasady zgłaszania prac i dostawy sprzętu

3.1 W celu zgłoszenia wykonania prac lub dostawy sprzętu w DC należy wysłać zgłoszenie na adres mailowy: awizacja@pnt.opole.pl co najmniej 24 godziny przed planowanym terminem prac. Zgłoszenie musi pochodzić z adresów mailowych,

wyszczególnionych na liście osób upoważnionych do kontaktów i autoryzacji lub z adresu wskazanego w umowie jako dane kontaktowe do współpracy.

3.2 Dyżurny Inżynier oraz ochrona obiektu każdorazowo dokonuje weryfikacji osób zgłaszających się do wykonania prac na terenie DC.

3.3 Jeśli osoba zgłaszająca się do wykonania prac nie ma wystarczających uprawnień, zgodnie z informacjami zawartymi w formularzu: Lista osób upoważnionych do kontaktów i autoryzacji, Dyżurny Inżynier nie wyda zgody na wykonanie prac. Jeśli weryfikacja zostanie potwierdzona, Dyżurny Inżynier udostępni odpowiednie pomieszczenia do wykonania prac.

3.4 Brak wcześniejszego zgłoszenia – w szczególnych przypadkach – spowodowanych np. wykonywanie zaplanowanych prac remontowych czy testów przez obsługę DC, może skutkować odmową dostępu lub koniecznością zmiany terminu prac przez Klienta (Podwykonawcę).

3.5 Dopuszcza się wykonywanie niezgłoszonych wcześniej prac jedynie w przypadku sytuacji awaryjnych jedynie przez osoby widniejące w formularzu: Lista osób upoważnionych do kontaktów i autoryzacji.

3.6 Jeśli osoba zgłaszająca dostawę nie ma wystarczających uprawnień do zgłoszenia dostaw, Dyżurny Inżynier wykona telefoniczną autoryzację zgłoszenia, potwierdzając zgłoszenie u osoby z prawem autoryzacji. Jeśli autoryzacja zostanie potwierdzona, Dyżurny Inżynier przyjmuje zgłoszenie

3.7 Jeśli autoryzacja nie powiedzie się, dostawa nie zostanie odebrana przez Dyżurnego Inżyniera.

3.8 Brak wcześniejszego zgłoszenia w szczególnych przypadkach, spowodowanych np. brakiem technicznych możliwości przyjęcia sprzętu, może skutkować odmową przyjęcia dostawy.

3.9 Przesyłki przyjmowane są na rampę rozładowczą DC. Nadawca ma obowiązek zapewnić odpowiedni sprzęt dla wyładunku dostawy na rampę.

3.10 Dopuszcza się przyjmowanie nie zgłoszonych wcześniej dostaw jedynie w przypadku sytuacji awaryjnych.

Należy wówczas jak najszybciej skontaktować się z Dyżurnym Inżynierem i zgłosić mu dostawę telefonicznie.

4. Zasady porządkowe

4.1 Zarządzenia porządkowe zebrane są „Zarządzeniach porządkowych obowiązujących w DATA CENTER".

4.2 Każdy Klient lub Podwykonawca zapoznaje się z zarządzeniami porządkowymi w ramach szkolenia przeprowadzonego przez Dyżurnego Inżyniera, co potwierdza na karcie szkolenia wstępnego podwykonawcy.

Park Naukowo-Technologiczny
w Opolu Sp. z o.o.
im. prof. Marka Tukiendorfa

PNT DATA CENTER

Kontakt

Wszystkie zgłoszenia związane z wykonywaniem prac, dostawami sprzętu czy dostępem do DC obsługuje Zespół Dyżurnych Inżynierów pracujących w trybie 24/7. Zespół Dyżurnych Inżynierów jest dostępny za pośrednictwem następujących kanałów komunikacji: telefon: +48 881 700 747, email: awizacja@pnt.opole.pl, https://support.pnt.cloud