

Akty prawne dot. wymagań na ochronę bezpieczeństwa teleinformatycznego i przetwarzanych informacji.

Ustawa z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2010 nr 182 poz. 1228 z pn. zm.) i pokrewne; Ustawa o ochronie informacji niejawnych określa zasady ochrony informacji, które stanowią tajemnicę państwową lub służbową. Przepisy ustawy mają zastosowanie do organów władzy publicznej, Sił Zbrojnych Rzeczypospolitej Polskiej i ich jednostek organizacyjnych, Narodowego Banku Polskiego i banków państwowych, państwowych osób prawnych, przedsiębiorców, jednostek naukowych lub badawczo-rozwojowych, których działalność związana jest z dostępem do informacji niejawnych. W szczególności Ustawa nakłada wymóg zapewnienia ochrony informacji niejawnych, w tym ich ochrony fizycznej; oraz zapewnienia ochrony systemów i sieci teleinformatycznych, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne. W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych m.in. należy wyznaczyć strefy bezpieczeństwa i zapewnić im kontrolę wejść/wyjść oraz kontrolę przebywania. Wymagane również jest stosowanie wyposażenia i urządzeń służącym ochronie informacji niejawnych, którym na podstawie odrębnych przepisów przyznano certyfikaty lub świadectwa kwalifikacyjne.

Dz.U. 2005 nr 171 poz. 1433 (z późn. zm.) Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego – organizacja ochrony bezpieczeństwa teleinformatycznego m.in. obejmuje ochronę fizyczną, elektromagnetyczną i kryptograficzną; zapewnienie niezawodności transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej.

Dz. Nr. 133,poz.883, (z późn. zm.) Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997r.

Dz.U. 2004 nr 100 poz. 1024 (z późn. zm.) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W rozporządzeniu zdefiniowane są poziomy bezpieczeństwa, wg których później określone są wymagania na środki bezpieczeństwa. Do środków bezpieczeństwa należą m.in. zabezpieczenie obszaru, w którym są przetwarzane dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności osób upoważnionych do przetwarzania danych osobowych; uwierzytelnianie użytkowników; zabezpieczenie przed awarią zasilania lub zakłóceniami w sieci zasilającej, kopie zapasowe .

Dz.U. 1997 nr 114 poz. 740 Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia.

Dz.U. 1998 nr 129 poz. 858 (z późn. zm.) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 14 października 1998 r. w sprawie szczegółowych zasad i wymagań, jakimi powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne.

Rozporządzenie do Ustawy o ochronie osób i mienia

Dz.U. 2002 nr 144 poz. 1204 Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną(z późn. zm.). Ustawa określa:

- 1) obowiązki usługodawcy związane ze świadczeniem usług drogą elektroniczną,
- 2) zasady wyłączania odpowiedzialności usługodawcy z tytułu świadczenia usług drogą elektroniczną,
- 3) zasady ochrony danych osobowych osób fizycznych korzystających z usług świadczonych drogą elektroniczną.

Zgodnie z Ustawą obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa podlegają obowiązkowej ochronie przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenie techniczne. Ponadto, ustawa określa:

- 1) obszary, obiekty i urządzenia podlegające obowiązkowej ochronie;
- 2) zasady tworzenia i funkcjonowania wewnętrznych służb ochrony;
- 3) zasady prowadzenia działalności gospodarczej w zakresie usług ochrony osób i mienia;
- 4) wymagane kwalifikacje i uprawnienia pracowników ochrony;
- 5) nadzór nad funkcjonowaniem ochrony osób i mienia;
- 6) zasady ochrony transportowanej broni, amunicji, materiałów wybuchowych, uzbrojenia, urządzeń i sprzętu wojskowego.

Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie. W szczególności określa wymagania na zabezpieczenia przeciwpożarowe.

Ustawa z dnia 18 lipca 2002 e. o świadczeniu usług drogą elektroniczną

Dz.U. 2004 nr 236 poz. 2364 Rozporządzenie Rady Ministrów z dnia 26 października 2004 r. w sprawie sposobu tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania dokumentów związanych z czynnościami bankowymi, sporządzanych na elektronicznych nośnikach informacji

Dz.U. 1991 nr 81 poz. 351 Ustawa z dnia 24 sierpnia 1991 r. o ochronie ppożarowej.

Dz.U. 2003 nr 116 poz. 1090

Rozporządzenie Rady Ministrów z dnia 24 czerwca 2003 r. w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony.

Autorzy programu zalecają, aby podczas prac projektowych oprócz wymagań prawnych stosować zalecenia norm oraz standardów celem zapewnienia jak najlepszych parametrów projektowanej serwerowni.

TIA - 942 TELECOMMUNICATIONS INFRASTRUCTURE STANDARD FOR DATA CENTERS
--

Standard amerykański opisujący zalecane rozwiązania dla Data Center przede wszystkim infrastrukturę kablową, schemat zabudowy serwerowni, ale również wymagania architektoniczne, wymagania dla instalacji elektroenergetycznej, klimatyzacji, systemu bezpieczeństwa fizycznego.

ASHRAE: DESIGN CONSIDERATION FOR DATACOMM EQUIPMENT CENTERS, 2005

Zalecenia wydane przez Amerykańskie Stowarzyszenie Inżynierów Ogrzewnictwa, Klimatyzacji i Wentylacji dotyczące budowy Data Center z naciskiem na schemat zabudowy serwerowni i scenariusze chłodzenia systemów komputerowych. Również podano zalecenia dla struktury budynku, parametrów środowiskowych, dostępności infrastruktury oraz ekonomicznego wykorzystania energii elektrycznej. Powyższy dokument jest podsumowaniem wcześniejszych prac komitetu ANSI/ASHRAE TC9.9: Thermal Guidelines for Data Processing Environments, 2005 oraz Datacom Equipment Power Trends and Cooling Applications, 2005.

INNE ZALECENIA, DOBRE PRAKTYKI I DOKUMENTY WHITE PAPERS

Ważnym źródłem zaleceń i dobrych praktyk związanych z budową Data Center są materiały wydawane przez amerykańskie organizacje zawodowe oraz producentów systemów informatycznych i infrastruktury wspierającej ich pracę:

1. AFCOM – stowarzyszenie działające od 25 lat, którego misją jest edukacja w zakresie nowych rozwiązań w Data Center tworzenie forum dla dzielenia się najlepszymi praktykami, trendami analizami pomiędzy wszystkimi zainteresowanymi stronami.
2. Dokumenty White Papers wydawane przez czołowych producentów infrastruktury wspierającej pracę urzędów IT: American Power Conversion oraz Emerson Network Power.

CZĄSTKOWE NORMY POLSKIE I EUROPEJSKIE

Większość przedstawionych w tym miejscu norm częściowych obowiązuje producentów materiałów i wyrobów stosowanych w budowie serwerowni. Omawianie tych norm ma wskazać gdzie należy poszukiwać określonych parametrów związanych z powszechnie stosowanymi klasyfikacjami materiałów i standardów wykonania prac budowlanych i instalacyjnych.

1. Modernizacja budowlana z przeznaczeniem na serwerownię
 - Ustawa z dnia 7 lipca 1994 r. – Prawo budowlane (Dz.U. z 1994 r. Nr 89 poz. 414 z późniejszymi zmianami)
 - Rozporządzenie Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. z 2002 r. Nr 75 poz. 690 z późniejszymi zmianami)
 - Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 25 kwietnia 2012 r. w sprawie szczegółowego zakresu i formy projektu budowlanego (Dz.U. z 2012 r. poz. 462)
 - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. z 2010 r. Nr 109 poz. 719)
 - Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (Dz.U. z 1997 r. Nr 129 poz. 844 z późniejszymi zmianami)

2. Instalacja elektroenergetyczna

- PN-IEC 60364 Instalacje elektryczne w obiektach budowlanych,
- PN-EN 12464-1:2004 Światło i oświetlenie – oświetlenie miejsc pracy – Część 1: Miejsce pracy we wnętrzach;
- PN-IEC 61024-1:2001 Ochrona odgromowa obiektów budowlanych – Zasady ogólne;
- PN-IEC 61024-1:2001 Ochrona odgromowa obiektów budowlanych – Zasady ogólne – Wybór poziomów ochrony dla urządzeń piorunochronnych;
- PN-IEC 60364-7-707:1999 Instalacje elektryczne w obiektach budowlanych – Wymagania dotyczące specjalnych instalacji lub lokalizacji – Wymagania dotyczące uziemnień instalacji urządzeń przetwarzania danych.
- PN-EN 62040-1-1:2006 Systemy bezprzerwowego zasilania (UPS) – Część 1-1: Wymagania ogólne i wymagania dotyczące bezpieczeństwa UPS stosowanych w miejscach dostępnych dla operatorów,
- PN-EN 62040-1-2:2005 Systemy bezprzerwowego zasilania (UPS) – Część 1-2: Wymagania ogólne i wymagania dotyczące bezpieczeństwa UPS stosowanych w miejscach o ograniczonym dostępie.
- PN-EN 62040-2:2006 System bezprzerwowego zasilania (UPS) – Część 2: Wymagania dotyczące kompatybilności elektromagnetycznej (EMC);
- Certyfikaty: ISO 9001: 2000 Quality managmentsystems – Requirements (odpowiednik krajowy: PN-EN ISO 9001:2001 Systemy zarządzania jakością – Wymagania)
ISO 14001:2004 Environmental management system – Requirements with giudance for use (odpowiednik krajowy: PN-EN ISO14001:2005 Systemy zarządzania środowiskowego – Wymagania I wytyczne stosowania).
- PN-93/T – 06450 Przemysłowe zakłócenia radioelektryczne – Urządzenia i metody pomiarów zakłóceń radioelektrycznych;
- PN-87/B - 02156 Akustyka budowlana – Metody pomiaru poziomu dźwięku A w Budynkach;
- PN-87/B – 02151.02 Akustyka budowlana – Ochrona przed hałasem pomieszczeń w budynkach – Dopuszczalne wartości poziomu dźwięku w pomieszczeniach;
- PN-EN 603000-3-1: 2005 Zarządzanie niezawodnością – Część 3-1: Przewodnik zastosowań – Techniki analizy niezawodności – Przewodnik metodologiczny;
- PN-EN 61078:2006 (U) Techniki analizy niezawodności – Metoda schematów blokowych niezawodności oraz metody boolowskie;
- PN-IEC 60300-3-4:2001 Zarządzanie niezawodnością – Przewodnik zastosowań – Przewodnik dotyczący specyfikowania wymagań niezawodnościowych.

3. Instalacja klimatyzacji i wentylacji

- PN-EN 12599:2002/AC:2004 Wentylacja budynków – Procedury badań i metody pomiarowe dotyczące odbioru wykonanych instalacji wentylacji i klimatyzacji;
- PN-76/B-03420 Wentylacja i klimatyzacja – Parametry obliczeniowe powietrza zewnętrznego;
- PN-EN 12599:2002, PN-EN 12599:2002/AC:2004 Wentylacja budynków – Procedury badań i metody pomiarowe dotyczące odbioru wykonanych instalacji wentylacji i klimatyzacji;

4. Instalacja teleinformatyczna

- PN-EN 50173-1:2004 Technika informatyczna – Systemy okablowania strukturalnego – Część 1: Wymagania ogólne i strefy biurowe;
- PN-EN 50174-1:2002 Technika informatyczna – Instalacja okablowania – Część 1: Specyfikacja i zapewnienie jakości,
- PN-EN 50174-2:2002 Technika informatyczna – Instalacja okablowania – Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków,
- PN-EN 50174-3:2005 Technika informatyczna – Instalacja okablowania – Część 3: Planowanie i wykonawstwo instalacji we wnętrzu budynków,
- PN-EN 50346:2004 Technika informatyczna – Instalacja okablowania – Badanie zainstalowanego okablowania,
- PN-EN 50310:2006 (U) Stosowanie połączeń wyrównawczych i uziemiających i uziemiających w budynkach z zainstalowanym sprzętem informatycznym;
- PN-EN 60825-2:2005 (U) Bezpieczeństwo urządzeń laserowych – Część 2: Bezpieczeństwo światłowodowych systemów telekomunikacyjnych;
- PN-EN 60950-1:2004 Urządzenia techniki informatycznej – Bezpieczeństwo – Część 1: Wymagania podstawowe;
- PN-EN 60950-21:2005 Urządzenia techniki informatycznej – Bezpieczeństwo – Część 21: zdalne zasilanie,
- PN-EN 41003:2001 Szczególne wymagania bezpieczeństwa dotyczące urządzeń przeznaczonych do podłączenia do sieci telekomunikacyjnych;

5. Zabezpieczenia przed podstawowymi zagrożeniami dla Data Center

Obowiązujące normy przedstawione poniżej, podzielone są na grupy odpowiadające podstawowym zagrożeniom:

- Pożarem.
- Włamaniem.
- Zalaniem wodą związaną z gaszeniem pożaru, kurzem, gazem lub dymem.
- Zakłóceniami elektromagnetycznymi i radiowymi.

6. Normy związane z zabezpieczeniem przed pożarem

- PN-EN 1047-1:2006 Pomieszczenia i urządzenia do przechowywania wartości – Klasyfikacja i metody badań odporności ogniowej – Część 1: szafy na nośniki danych i wkładki na dyskietki;
- PN-EN 1047-2:2002 Pomieszczenia i urządzenia do przechowywania wartości – Klasyfikacja i metody badań odporności ogniowej – Część 2: Pomieszczenia oraz pojemniki do przechowywania nośników informacji;
- PN-EN 1363-1:2001 Badania odporności ogniowej – Część 1: Wymagania ogólne;
- PN-EN 1363-2:2001 Badania odporności ogniowej – Część 2: Procedury alternatywne i dodatkowe;
- PN-EN 54-2:2002/A1:2007 (U) Systemy sygnalizacji pożarowej - Część 2: Centrale sygnalizacji pożarowej;
- PN-EN 54-3:2003/A2:2006 (U) Systemy sygnalizacji pożarowej – Część 3: Pożarowe urządzenia alarmowe – Sygnalizatory akustyczne;
- PN-EN 54-4:2001/A2:2006 (U) Systemy sygnalizacji pożarowej – Część 4: Zasilacze;
- PN-EN 54-4:2003 Systemy sygnalizacji pożarowej – Część 5: Czujki ciepłe – Czujki punktowe;

- PN-EN 54-7:2004/A2:2006 (U) Systemy sygnalizacji pożarowej – Część 7: Czujki dymu – Czujki punktowe działające z wykorzystaniem światła rozproszonego, światła przechodzącego lub jonizacji;
 - PN-EN 54-11:2004/A1:2006 Systemy sygnalizacji pożarowej – Część 11: Ręczne ostrzegawcze pożarowe;
 - PN-EN 54-20:2006 (U) Systemy sygnalizacji pożarowej – Część 20: Czujki dymu zasysające;
 - PN-EN 54-21:2006 (U) Systemy sygnalizacji pożarowej – Część 21: Urządzenia do transmisji sygnałów alarmowych i uszkodzeniowych;
 - ISO 14520 – 1, -5, -14 Gazowe systemy gaśnicze – Właściwości fizycznej projektowanie
7. Normy związane z zabezpieczeniem przed włamaniem oraz z Elektronicznych Systemów Ochrony (ESO).
- PN-EN 1143-1:2006 Pomieszczenia i urządzenia do przechowywania wartości – Wymagania, klasyfikacji metody badań odporności na włamanie – Część 1: Szafy, szafy ATM, pomieszczenia i drzwi do pomieszczeń,
 - PN-EN 1300:2006 Pomieszczenia i urządzenia do przechowywania wartości – Klasyfikacja zamków o wysokim stopniu zabezpieczenia z punktu widzenia odporności na nieuprawnione otwarcie,
 - PN-E 08390-14:1993 Systemy alarmowe – Wymagania ogólne – Zasady stosowania,
 - PN-93/E-08390 „Systemy alarmowe – Włamaniowe systemy alarmowe”.
 - PN-EN 50131 „Systemy alarmowe – Systemy sygnalizacji włamania i napadu”
 - PN-EN 50136 „Systemy alarmowe – systemy i urządzenia transmisji alarmu”;
 - PN-EN 50133 „Systemy alarmowe – Systemy kontroli dostępu”;
 - PN-EN 50132 „Systemy alarmowe – Systemy dozoru CCTV w zastosowaniach dotyczących zabezpieczenia”
 - PN-EN 50130-4:2002/A2:2007 Systemy alarmowe – Część 4: Kompatybilność elektromagnetyczna – Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów alarmowych pożarowych, włamaniowych i osobistych.
8. Normy związane z zabezpieczeniem przed zalaniem wodą związaną z gaszeniem pożaru, kurzem, gazem lub dymem.
- PN-EN 1634-3:2006/AC:2006 Badania odporności ogniowej zestawów drzwiowych i żaluzjowych – Część 3: Sprawdzanie dymoszczelności drzwi i żaluzji;
 - PN-EN 60529:2003 Stopnie ochrony zapewnianej przez obudowy (Kod IP);
9. Normy związane z zabezpieczeniem przed zakłóceniami, elektromagnetycznymi i radiowymi.
- PN-EN 55024:2000, PN-EN 55024:2000/A1:2002 (U), PN-EN 55024:2000/A1:2004, PN-EN 55024:2000/A2:2004 Kompatybilność elektromagnetyczna (EMC) – Urządzenia informatyczne – Charakterystyki odporności – Metody pomiaru i dopuszczalne poziomy.