

Partner IT



„Certyfikat Bezpieczeństwa Związku Powiatów Polskich”



	Strona
O NAS	3
AUDIT CERTYFIKUJĄCY	6
AUDIT WERYFIKACYJNY	10
ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI	11
POLITYKA BEZPIECZEŃSTWA INFORMACJI	12
INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM	13
CERTYFIKAT BEZPIECZEŃSTWA ZWIĄZKU POWIATÓW POLSKICH	14
CERTYFIKAT - NORMA ISO/IEC 27001:2005	16
CERTYFIKAT – NORMA PN-EN ISO 9001:2009 (ISO 9001:2008)	17
CERTYFIKAT ISO – NORMA ISO 14001:2004	19
INTEGRACJA SYSTEMÓW	20
SZKOLENIA WEWNĘTRZNE	21
• Szkolenia dla pracowników Jednostek Samorządu Terytorialnego	
SZKOLENIA ZEWNĘTRZNE	22
• Wdrożenie Systemu Zarządzania Jakością wg PN-EN ISO 9001:2009 (ISO 9001:2008) w praktyce	
•	
• Auditor wewnętrzny / pełnomocnik Systemu Zarządzania Jakością wg normy ISO 9001:2008	
• Auditor wewnętrzny ISO 14001	
• Auditor / Pełnomocnik Zintegrowanego Systemu Zarządzania wg. norm ISO 9001, 14001	
• Auditor / Pełnomocnik Systemu Zarządzania Bezpieczeństwem Informacji	

O NAS

Amigable.pl Sp. z o.o., 00-608 Warszawa, al. Niepodległości 186, KRS 0000264094, NIP 7010055029 jako partner technologiczny Związku Powiatów Polskich jest jedynym podmiotem uprawnionym do prowadzenia auditów weryfikujących działania Jednostek Samorządu Terytorialnego w zakresie bezpieczeństwa przetwarzania danych osobowych i systemu informatycznego w świetle zgodności z obowiązującymi przepisami pozwalających uzyskać „**Certyfikat Bezpieczeństwa Związku Powiatów Polskich**” – **350 punktów w rankingu Związku Powiatów Polskich.**

Nasze działania nie prowadzą jedynie do stwierdzenia stanu faktycznego w jednostce, jak w przypadku klasycznego auditu, ale stanowią partnerską współpracę nawiązaną poprzez podpisanie pierwszej umowy z możliwością jej kontynuacji przez wiele lat. Oferujemy Państwu również swoją pomoc w zakresie doradztwa, w jaki sposób najkorzystniej usunąć ewentualne niedociągnięcia. W ramach naszej działalności zapewniamy poufność informacji - wszelkie informacje o Państwa jednostce są u nas objęte **Tajemnicą.**

Współpraca z Amigable.pl gwarantuje:

- niezależność naszej firmy jako auditora zewnętrznego;
- pełny zakres obsługi technicznej i szkoleniowej;
- najwyższą jakość usług gwarantowaną przez Związek Powiatów Polskich.

Szanowni Państwo,

jako partner technologiczny **Związku Powiatów Polskich** codziennie realizujemy zadania podnoszące sprawność i budujące bezpieczeństwo **Jednostek Samorządu Terytorialnego**.

Jesteśmy jedynym podmiotem uprawnionym do realizacji projektu "**Certyfikat Bezpieczeństwa Związku Powiatów Polskich**".

Wykonanie przez nas auditu certyfikującego gwarantuje Jednostce otrzymanie Certyfikatu Bezpieczeństwa Związku Powiatów Polskich.

Przedmiotem certyfikacji objęta jest infrastruktura informatyczna, gdzie badamy wszystkie zabezpieczenia zarówno na poziomie serwerów jak i stacji roboczych. Dlatego też auditor odwiedza każdego pracownika na stanowisku pracy indywidualnie. Dodatkowym efektem prowadzonych działań jest inwentaryzacja sprzętu i oprogramowania, która dokonywana jest jakby przy okazji naszych działań.

Wszystkie nasze działania wpływają na podświadomość pracowników i uzmysławiają im, że w każdej chwili ich działania prowadzone w godzinach pracy mogą zostać zweryfikowane.

Równocześnie auditowi podlega cała dokumentacja w zakresie ochrony danych. W ramach certyfikatu mieści się również ochrona fizyczna budynku tj. zabezpieczenia oraz dokumentacja do nich tworzona.

Wszystkie prowadzone przez nas działania są zgodne z normą ISO/IEC 27001:2005. Oznacza to, że wszystkie wykonywane przez nas czynności przybliżają Urząd do certyfikacji z zakresu w/w normy.

Gwarantujemy pełną poufność. Na miejscu przed przystąpieniem do realizacji umowy auditorzy podpisują stosowne oświadczenia gwarantujące Państwu pełne bezpieczeństwo.

Warto podkreślić iż przystąpienie do Certyfikacji (Certyfikat Bezpieczeństwa Związku Powiatów Polskich) nie wymaga żadnych specjalnych przygotowań ze strony Urzędu. Dzięki wizycie auditorów na miejscu w Urzędzie istnieje możliwość błyskawicznego usunięcia ewentualnych uchybień. Nie ma też obawy iż jakiekolwiek informacje zdobyte podczas auditu wydostaną się poza mury Urzędu bowiem obowiązuje nas zachowanie tajemnicy czego potwierdzeniem jest dokument podpisywany na miejscu w Urzędzie.

Certyfikat Bezpieczeństwa Związku Powiatów Polskich to nie tylko bezpieczeństwo Urzędu ale przede wszystkim gwarancja spokoju dla Kierownictwa Jednostki, które bezpośrednio odpowiada karnie za nieprawidłowości w jednostce.

W celu uzyskania przez Urząd Certyfikatu Bezpieczeństwa Związku Powiatów Polskich konieczne jest przeprowadzenie przez nas auditu certyfikującego polegającego na przeglądzie pełnej dokumentacji Urzędu, planów przeciwpożarowych, archiwum zakładowego, weryfikacji zbiorów zgłoszonych do GIODO. Działania informatyczne mają na celu zapewnienie Państwu w przyszłości bezpieczeństwa i ciągłości pracy jednak przede wszystkim dadzą Państwu spojrzenie na to jak pracownicy reagują na zagrożenia z zewnątrz i czy są podatni na ingerencje osób trzecich.

W odróżnieniu od klasycznego auditu nasza obecność w Urzędzie przynosi natychmiastową korzyść ponieważ wszędzie tam gdzie jest taka możliwość staramy się uzupełniać bądź aktualizować dokumentację.

Jako partner technologiczny Związku Powiatów Polskich jesteśmy jedynym podmiotem uprawnionym do wystawiania Certyfikatu Bezpieczeństwa Związku Powiatów Polskich (350 pkt. w rankingu ZPP) po przeprowadzonym audicie.

Oprócz certyfikatu Bezpieczeństwa Związku Powiatów Polskich przygotowujemy także Urzędy do Certyfikacji **ISO/IEC 27001:2005**.

Mając na względzie kompleksowość proponowanych przez nas rozwiązań oprócz auditu sugerujemy przeprowadzenie także praktycznego szkolenia dla wszystkich pracowników Urzędu z ochrony danych osobowych. Ponieważ ściśle współpracujemy z samorządami, realizujemy audyty, przygotowujemy dokumenty w postaci Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem mamy doświadczenie, które pozwala nam przeprowadzić specjalistyczne szkolenie bazujące na konkretnych przykładach a nie cytować zapisy ustaw. Takie podejście sprawia, że przekazywana przez nas wiedza jest dobrze odbierana i w pełni zrozumiała dla wszystkich pracowników.

Na stronie www.bezpieczenstwo.org/referencje.html publikowane są referencje od Urzędów, które m.in. odwiedziliśmy.

Więcej informacji na stronie: www.bezpieczenstwo.org/bezpieczenstwo_jst.html

KONTAKT

+48 693 34 64 20

+48 22 490 53 20

bezpieczenstwo@zpp.pl

www.bezpieczenstwo.org

AUDIT CERTYFIKUJĄCY – 350 punktów w rankingu ZPP

Audit pozwalający uzyskać „Certyfikat Bezpieczeństwa Związku Powiatów Polskich” jest kompletnym auditem polegającym na uzupełnieniu przez auditorów wszystkich uchybień występujących w Urzędzie w zakresie „Certyfikatu Bezpieczeństwa Związku Powiatów Polskich”.

Ochrona legalności oprogramowania

W ramach auditu certyfikującego mieści się pełen audit legalności oprogramowania. W przypadku stwierdzenia pełnej legalności, niezależnie od Certyfikatu Bezpieczeństwa Związku Powiatów Polskich Jednostka może otrzymać Certyfikat Legalności Microsoft. W ramach auditu certyfikującego wdrażane są zasady zarządzania oprogramowaniem poprzez powołanie osoby zarządzającej oprogramowaniem, wykonanie metryk każdego komputera jak i wprowadzenie porozumień pomiędzy kierownikiem jednostki a każdym użytkownikiem komputera, przenoszących odpowiedzialność karną kierownika jednostki za stan legalności oprogramowania na pracownika.

Proponowane podczas auditu rozwiązania pozwalają uchronić Urząd przed interwencją Policji, polegającą na zabezpieczeniu (zabraniu) komputerów jako narzędzi przestępstwa (co faktycznie ma miejsce), a także ustrzec przed odpowiedzialnością wynikającą z kodeksu karnego.

Audit w zakresie legalności oprogramowania polega na:

- sprawdzeniu 100% dostępnych komputerów w zakresie przestrzegania przez urząd Ustawy o ochronie praw autorskich i praw pokrewnych,
- wdrożeniu zasad zarządzania oprogramowaniem,
- przeniesieniu odpowiedzialności prawnej i karnej z kierownictwa Jednostki na użytkowników komputerów poprzez wdrożenie stosownych dokumentów,
- Audit pozwala na usunięcie zbędnych programów, często zainstalowanych niezgodnie z warunkami licencji.
- Audit ułatwia właściwy zakup oraz zapewnia pełną kontrolę kosztów związanych z zakupem oprogramowania.
- z pełnym zestawieniem ilości posiadanych i zainstalowanych licencji.

Ochrona komputerów i sieci

W ramach auditu certyfikującego mieści się pełen audit stanu bezpieczeństwa komputerów i sieci oraz odporności na zagrożenia wewnętrzne i zewnętrzne. Podczas auditu wyszukiwane jest m.in. oprogramowanie szpiegowskie umożliwiające kradzież danych Jednostki poprzez Internet.

Audit w zakresie bezpieczeństwa komputerów i sieci polega na:

- pełnej weryfikacji stanu bezpieczeństwa sieci komputerowej w Jednostce,
- ustaleniu, przy współpracy ze służbami informatycznymi, zasad prawidłowego zarządzania kontami użytkowników,

- określeniu standardu zabezpieczeń i zdefiniowaniu polityki zarządzania uprawnieniami i hasłami dostępu,

Wdrożenie procedur ochrony komputerów i sieci zabezpiecza infrastrukturę Jednostki, ochroni przed atakami z zewnątrz i z wewnątrz, zapewnia używanie właściwych, bezpiecznych hasel oraz wprowadza pełną ochronę fizyczną i programową stanowisk komputerowych.

Ochrona danych osobowych

Pełen audit polega na analizie obowiązujących aktów prawa wewnętrznego wydanych przez kierownika JST pod kątem ich zgodności z obowiązującym stanem prawnym oraz wymogami określonymi w Polskich Normach, na dzień prowadzonego auditu. Analizie poddawane są zarządzenia oraz załączniki do tych zarządzeń wydane w celu realizacji przepisów aktów normatywnych, tj.:

- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jednolity z 2002r. Dz. U. Nr 101, poz. 926 z późniejszymi zmianami),
- Ustawa o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994r. (tekst jednolity z 2006r, Dz. U. Nr 90 poz. 631 z późniejszymi zmianami),
- Ustawa o narodowym zasobie archiwalnym i archiwach z dnia 14 lipca 1983r. (tekst jednolity z 2006r. Dz. U. Nr 97, poz. 673 z późniejszymi zmianami),
- Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z 17 lutego 2005r. (Dz. U. Nr 64, poz. 565 z późniejszymi zmianami)

oraz wydanymi na podstawie powyższych aktów, przepisów wykonawczych tj.:

- Rozporządzenie Rady Ministrów w sprawie minimalnych wymagań dla systemów teleinformatycznych z dnia 11 października 2005r. (Dz. U. Nr 212 poz. 1766),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004r (Dz. U. Nr 100, poz. 1024),
- Rozporządzenie Ministra Kultury w sprawie warunków przechowywania dokumentacji osobowej i płacowej pracodawców z dnia 15 lutego 2005r. (Dz. U. Nr 32 poz. 284),
- Rozporządzenie Ministra Kultury w sprawie określenia rodzaju wykształcenia uznanego za specjalistyczne oraz dokumentów potwierdzających posiadanie praktyki zawodowej, wymaganych od osób wykonujących niektóre czynności związane z dokumentacją osobową i płacową pracodawców z dnia 1 kwietnia 2005r. (Dz. U. Nr 68 poz. 596),
- Rozporządzenia Ministra Kultury w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych z dnia 16 września 2002r. (Dz. U. Nr 167, poz. 1375).

Na podstawie wyników uzyskanych z analizy istniejącego stanu prawnego w urzędzie, przeprowadzone są czynności polegające:

- na opracowaniu wszystkich brakujących zarządzeń wprowadzających dokumentację oraz procedur postępowania, regulujących bezpieczeństwo przetwarzanych danych w urzędzie zgodnie z obowiązujących unormowaniami prawnymi. Opracowane materiały są przekazywane w stanie gotowym do podpisu przez kierownika JST i natychmiastowego wdrożenia,

- na wskazaniu odpowiednich osób do powierzenia im obowiązków Administratora Bezpieczeństwa Informacji oraz Administratora sieci oraz opracowaniu prawidłowej dokumentacji do ich powołania.

Dokonywana jest analiza aktów prawnych takich jak:

- Instrukcja kancelaryjna obiegu dokumentów,
- Instrukcja obiegu dokumentów księgowych,
- Zarządzenie w sprawie ochrony danych osobowych,
- Procedury dotyczące ochrony danych.

Ustala się czy w jednostce:

- wytwarzane są lub przechowywane dokumenty o charakterze niejawnym,
- czy są osoby posiadające poświadczenie bezpieczeństwa,
- gdzie i jak przechowywane są dokumenty oraz jak prowadzona jest ich ewidencja.

Sprawdzone jest czy:

- wyznaczono Administratora Bezpieczeństwa Informacji i jaki jest jego zakres obowiązków,
- powołanie ABI nastąpiło zgodnie z wymogami prawa,
- osoba będąca ABI przestrzega obowiązki wynikające z ustawy.

Dokonywane jest przeglądanie zbiorów pod kątem obowiązku rejestracji

- Zbiory zgłoszone
- Zbiory tymczasowe
- Zbiory do zgłoszenia

Sprawdzone jest zabezpieczenie danych podczas ich przetwarzania

- Stan biurka
- Sposób zabezpieczenia wyświetlanych na monitorze danych
- Kontrola dostępu do danych (komputer, szafy, pomieszczenia)

Weryfikuje się czy archiwum Jednostki spełnia wymogi prawa. Dokonywana jest:

- ocena wykazu akt i stosowanych procedur archiwizacji,
- ocena pomieszczeń, ich zabezpieczenia, dostępu, itp.
- analiza procedur niszczenia dokumentów (również stanowiskowych).

Wdrożenie procedur ochrony danych osobowych zapewnia przestrzeganie przez jednostkę "Ustawy o ochronie danych osobowych" z wszystkimi nowelizacjami.

Wszystkie działania mają na celu zminimalizowanie odpowiedzialności kierownictwa na wypadek „nieprzyjemnej” kontroli Głównego Inspektora Danych Osobowych.

UWAGA: Kontrole GIODO są coraz częstsze, wywołane zazwyczaj złożoną skargą bądź to przez niezadowolonego petenta bądź przez pracownika, który został zwolniony.

Bezpieczeństwo Fizyczne i Środowiskowe

Pełen audit bezpieczeństwa fizycznego i środowiskowego polega na porównaniu istniejącego stanu bezpieczeństwa Urzędu z wymogami wskazanymi w Polskich Normach w zakresie bezpieczeństwa pożarowego, energetycznego oraz instalacji alarmowej, a także z obowiązującym stanem prawnym, w szczególności:

- Ustawa o ochronie przeciwpożarowej z dnia 24 sierpnia 1991r (tekst jednolity z 2002 roku Dz. U. Nr 147 poz. 1229 z późniejszymi zmianami),
- Prawo budowlane z dnia 7 lipca 1994r. (tekst jednolity z 2006 roku Dz. U. Nr 156 poz. 1118 z późniejszymi zmianami),

oraz wydanymi na podstawie powyższych aktów, przepisami wykonawczymi tj.:

- Rozporządzenie Ministra Infrastruktury z 12 kwietnia 2002r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. Nr 75, poz. 690),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów z dnia 21 kwietnia 2006r. (Dz. U. Nr 80 poz. 563).

W oparciu o powyższe przepisy prawne przeprowadza się czynności, których celem jest:

- ocena stanu zabezpieczenia antywłamaniowego w Urzędzie
- ocena dokumentacji z zakresu bezpieczeństwa pożarowego w świetle obowiązujących przepisów o ochronie przeciwpożarowej,
- ocena dokumentacji związanej z ochroną obiektu oraz ewakuacją Urzędu w sytuacjach zagrażających bezpieczeństwu,
- ocena zgodności stanu lokalu archiwum zakładowego i serwerowni, warunków jego wyposażenia w świetle wymogów określonych w przepisach prawnych dla tego rodzaju pomieszczeń i wskazanie stwierdzonych niezgodności
- ocena bezpieczeństwa energetycznego obiektu w zakresie zasilania podstawowego i rezerwowego.
- wskazanie słabych punktów w zabezpieczeniu fizycznym obiektu.
- opracowanie brakujących zarządzeń wprowadzających dokumentację regulującą postępowanie oraz zachowanie pracowników w kierunku podniesienia bezpieczeństwa Urzędu oraz pomoc przy opracowaniu dokumentów związanych z bezpieczeństwem fizycznym obiektu.

Podczas auditu certyfikującego audytorzy Amigable.pl zostawiają gotowe dokumenty (zarządzenia, rozporządzenia i upoważnienia, które należy tylko wprowadzić w Jednostce) oraz spis oprogramowania, które należy zweryfikować pod względem licencji (w przypadku wykazania braków należy dokonać zakupu lub usunąć nielegalne oprogramowanie z komputerów, aby pozostać w zgodzie z ustawą o prawach autorskich i prawach pokrewnych).

AUDIT WERYFIKACYJNY

Dla Kierowników Jednostek Samorządu Terytorialnego audit jest szansą odciążenia się od odpowiedzialności karnej za dotychczasowy stan Urzędu (bez względu na fakt czy jest to pierwsza czy druga kadencja). Jest to szczególnie ważne i istotne w przypadku nieprawidłowości dotyczących przetwarzania danych osobowych i braku legalności oprogramowania, za co karne odpowiada Kierownik jednostki.

Audit weryfikujący stanu bezpieczeństwa urzędu polega na:

- sprawdzeniu ok. 10-20% komputerów w zakresie przestrzegania przez urząd Ustawy o ochronie praw autorskich i praw pokrewnych,
- ogólnej weryfikacji stanu bezpieczeństwa sieci komputerowej w jednostce,
- weryfikacji przestrzegania przez urząd Ustawy o ochronie danych osobowych wraz z Ustawą o archiwach państwowych
- weryfikacji stanu bezpieczeństwa fizycznego jednostki.

Audity Amigable.pl są zawsze przyjazne dla jednostki auditowanej. Każdy audit kończy się raportem o stanie bezpieczeństwa urzędu (wykonany przez zewnętrznego audytora).

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

Informacje to cenny zasób każdej organizacji, bez względu na to, czy są one drukowane na papierze, przechowywane w formie elektronicznej, wysyłane pocztą czy transmitowane za pośrednictwem nowoczesnych środków komunikacji.

Aby efektywnie zarządzać zagrożeniami i czynnikami ryzyka w zakresie polityki ochrony informacji w organizacji, należy wdrożyć odpowiedni System Zarządzania Bezpieczeństwem Informacji.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

– 350 punktów w rankingu ZPP

Polityka Bezpieczeństwa Informacji jest podstawowym i zasadniczym dokumentem bezpieczeństwa w Jednostce Samorządu Terytorialnego. W dokumencie tym zawarte są definicje podstawowych celów bezpieczeństwa, specyfika zasad bezpieczeństwa oraz definicja infrastruktury organizacyjnej. Odpowiednio opracowana i wdrożona jest jednym z kluczowych elementów, stanowiących filar bezpieczeństwa. Określa podejście instytucji do zarządzania bezpieczeństwem informacji i dzięki zaangażowaniu czynników decyzyjnych w danej instytucji, pozwala na praktyczne jej wdrożenie w odniesieniu do wszystkich pracowników poprzez jasne określenie obowiązujących celów i zasad bezpieczeństwa informacji. Wdrożenie Polityki Bezpieczeństwa Informacji obejmuje szeroki zakres działań i mechanizmów, takich jak szkolenia, budowanie świadomości bezpieczeństwa pracowników, wdrożenia odpowiednich technologii.

Zasadnicza wartość Polityki Bezpieczeństwa Informacji jest związana z jej charakterem jako dokumentu zarządczego, odzwierciedlającego postrzeganie i zaangażowanie kierownictwa organizacji w sprawach związanych z bezpieczeństwem informacji. Dokument ten jest tworzony we współpracy z pracownikami jednostki i jest akceptowany przez jej zarząd, a tym samym obowiązuje wszystkich pracowników organizacji.

Amigable.pl Sp. z o.o. proponuje usługi związane ze stworzeniem Polityki Bezpieczeństwa Informacji od podstaw lub przy uwzględnieniu istniejących już dokumentów i uregulowań.

Polityka Bezpieczeństwa Informacji jest specjalnie tworzona i dostosowywana dla każdej jednostki, z uwzględnieniem środowiska technologicznego i charakterystycznej specyfiki działania.

Stworzona Polityka Bezpieczeństwa Informacji będzie spełniać następujące cele:

- Dostarczać pracownikom organizacji wskazówek w zakresie bezpieczeństwa informacji;
- Wspierać kierownictwo w zakresie utrzymania odpowiedniego poziomu bezpieczeństwa organizacji;
- Ustalać najważniejsze standardy bezpieczeństwa informacji;
- Definiować role i zakresy odpowiedzialności w organizacji;
- Wpływać na budowanie świadomości bezpieczeństwa wśród pracowników i kierownictwa;
- Określać ramy dla głównych procesów roboczych dotyczących bezpieczeństwa informacji;
- Służyć jako podstawa dla ustanowienia procedur bezpieczeństwa.

Podstawowym mechanizmem służącym wdrożeniu Polityki Bezpieczeństwa Informacji jest stworzenie kompleksowego zestawu Procedur Bezpieczeństwa Informacji, który pozwala na wykorzystanie Polityki Bezpieczeństwa Informacji jako dokumentu operacyjnego i przynoszącego realne korzyści dla Urzędu. Prawidłowo stworzony zestaw Procedur jest nieodzownym i podstawowym środkiem wdrażania Polityki Bezpieczeństwa Informacji.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Jednym z podstawowych mechanizmów wdrażania Polityki Bezpieczeństwa Informacji jest wdrożenie Instrukcji Zarządzania Systemem Informatycznym. Poprawna realizacja zadań związanych z ochroną zasobów informacyjnych wymaga wdrożenia, opartej o odpowiednie normy i uwzględniającego regulacje prawne dotyczące poszczególnych obszarów (jak bezpieczeństwo danych osobowych, bezpieczeństwo fizyczne, zgodność z ustawami).

Prawidłowo stworzone i wdrożone Procedury regulują procesy związane z bezpieczeństwem i przyczyniają się do budowania świadomości bezpieczeństwa w organizacji.

Niezmiernie istotną rolą Procedur jest pewność, że działania bezpieczeństwa są faktycznie realizowane i nie pozostają jedynie wymogiem teoretycznym, a także iż Procedury stanowią podstawę do ciągłej kontroli poprawności działań związanych z ochroną zasobów informacyjnych przedsiębiorstwa. Dzięki wprowadzeniu procedur możliwa staje się realizacja działań związanych z bezpieczeństwem informacji w sposób jednolity, poprzez wprowadzenie standaryzacji procesów i zachowań.

Amigable.pl Sp. z o.o. proponuje usługi związane ze stworzeniem zestawu Procedur Bezpieczeństwa Informacji od podstaw lub przy uwzględnieniu istniejących już dokumentów i uregulowań.

Każdorazowo zestaw procedur tworzony jest z uwzględnieniem istniejących rozwiązań w danej organizacji oraz ze wskazaniem zawartymi w stosownych normach dotyczących zarządzania bezpieczeństwem informacji i bezpieczeństwa systemów informatycznych.

CERTYFIKATY

CERTYFIKAT BEZPIECZEŃSTWA ZWIĄZKU POWIATÓW POLSKICH – 350 punktów w rankingu

Dzięki odpowiedniej ochronie informacji, jej użytkownicy mogą być pewni, że zachowane zostały najważniejsze elementy stanowiące o jej przydatności:

- **Poufność** – gwarantująca dostęp do określonych informacji tylko osobom do tego upoważnionym;
- **Integralność** – zapewniająca dokładność i kompletność zarówno samej informacji jak i metod, za pomocą których jest przetwarzana;
- **Dostępność** – gwarantująca uprawnionym osobom dostęp do informacji w czasie, gdy jest ona wymagana.

Aby informacja mogła spełniać powyższe kryteria, konieczne jest zastosowanie szeregu działań i mechanizmów zarówno z zakresu infrastruktury technicznej, jak i organizacyjnej. Działania te mają na celu zminimalizowanie istniejącego dla danej Jednostki Samorządu Terytorialnego ryzyka związanego z utratą poufności, integralności i dostępności zasobów informacyjnych.

Niezwykle istotnym czynnikiem bezpieczeństwa systemu informacyjnego jest regularne wykonywanie auditów bezpieczeństwa, zarówno w aspekcie fizycznym jak i informatycznym. Dzięki wykonaniu kompleksowego audytu bezpieczeństwa w oparciu o Polskie Normy i odpowiednie ustawy, możliwe jest zbadanie aktualnego stanu zabezpieczeń oraz przedstawienie zaleceń w zakresie zarządzania bezpieczeństwem informacji. Audit infrastruktury informatycznej jest ważnym elementem i podstawą do podjęcia prac związanych z odpowiednim zabezpieczeniem technologicznym, funkcjonalnym i proceduralnym Urzędu.

Należy jednocześnie zaznaczyć, że tylko wykonanie przez Amigable.pl Sp. z o.o., 00-608 Warszawa, al. Niepodległości 186, KRS 0000264094, NIP 7010055029 Audytu certyfikującego, gwarantuje bezpieczeństwo przetwarzania danych i pozwala na otrzymanie przez Jednostkę Samorządu Terytorialnego Certyfikatu Bezpieczeństwa Związku Powiatów Polskich.

W ramach prowadzonych auditów certyfikujących sprawdzamy bezpieczeństwo systemów informatycznych. W zależności od sytuacji, dokonujemy wdrożenia procedur bezpieczeństwa poprzez wprowadzenie stosownych zabezpieczeń chroniących system przed dostępem osób nieupoważnionych a w konsekwencji możliwą utratą danych. Weryfikujemy przestrzeganie przez Urząd, Ustawy o ochronie danych osobowych w zakresie przetwarzania danych zarówno w formie papierowej jak i elektronicznej. Nasi specjaliści wykonują również wdrożenie bezpieczeństwa fizycznego jednostki sprawdzając wszelkie zabezpieczenia, jakie winny być zastosowane w celu uniemożliwienia wtargnięcia osób postronnych na teren jednostki jak i urządzeń technicznych zapewniających ciągłość pracy na wypadek zdarzeń losowych.

Korzyści wynikające z otrzymania certyfikatu

- Gwarancja spełnienia przez Urząd wymogów Ustawy o prawie autorskim i prawach pokrewnych oraz Ustawy o ochronie danych osobowych,
- Na pisemny wniosek Jednostki następuje wpisanie do bazy bezpiecznych urzędów w Polsce, która jest udostępniana organom kontrolnym i ścigania.

- Rejestracja w bazie może spowodować odstąpienie organu od wykonania czynności kontrolnych,
- 350 punktów w rankingu prowadzonym przez Związek Powiatów Polskich.

Po otrzymaniu certyfikatu jednostka otrzymuje nieodpłatnie wszelkie aktualizacje i nowelizacje, jakie w okresie certyfikacji wydaje organ ustawodawczy, a które wymagają wprowadzenia w jednostce samorządu terytorialnego.

Certyfikat jest ważny rok od momentu jego wydania.

Istnieje możliwość przedłużenia ważności certyfikatu na kolejne lata.

CERTYFIKAT - NORMA ISO/IEC 27001:2005 – 1050 punktów w rankingu ZPP

Informacja ma zasadnicze znaczenie dla podejmowanych działań, a może nawet dla przetrwania organizacji. Certyfikat ISO/IEC 27001 pomaga w zarządzaniu cennymi zasobami informacji i chronieniu ich.

System Zarządzania Bezpieczeństwem Informacji, bazujący na założeniach międzynarodowych norm ISO/IEC 27001:2005, pomoże Państwu we wdrożeniu efektywnej struktury umożliwiającej stosowanie i ciągłe udoskonalanie mechanizmów bezpieczeństwa informacji oraz zarządzanie nimi.

ISO/IEC 27001 to jedyna poddawana audytom norma międzynarodowa, która określa wymogi dotyczące Systemów Zarządzania Bezpieczeństwem Informacji. Norma ta została opracowana w celu zapewnienia wyboru adekwatnych i proporcjonalnych środków bezpieczeństwa.

Pomaga to w ochronie zasobów informacji i daje pewność wszystkim zainteresowanym stronom, w szczególności Państwa klientom. Norma jest oparta na procesowej metodzie ustanawiania, wdrażania, obsługiwania, monitorowania, badania, utrzymywania i usprawniania Państwa Systemu Zarządzania Bezpieczeństwem Informacji.

Norma ISO/IEC 27001 dotyczy każdej organizacji, dużej i małej, z dowolnej branży i dowolnej części świata. Norma ta jest szczególnie przydatna tam, gdzie ochrona informacji ma znaczenie zasadnicze, na przykład w sektorach finansów, opieki medycznej, publicznym i informatycznym.

Norma ISO/IEC 27001 jest także efektywna w przypadku organizacji, które zarządzają informacjami w czyimś imieniu, na przykład podwykonawców usług informatycznych. Może służyć do zapewnienia klientów, że ich informacje są odpowiednio chronione.

Certyfikat ISO/IEC 27001:2005:

- stanowi niezależną gwarancję wewnętrznych narzędzi kontroli i spełnia wymogi zarządzania korporacyjnego i ciągłości działania;
- stanowi niezależne potwierdzenie przestrzegania odpowiednich przepisów i prawa;
- podnosi konkurencyjność, ponieważ jest zgodna z wymogami kontraktów, i przekonuje klienta, że bezpieczeństwo jego informacji jest Państwa celem nadrzędnym;
- niezależnie weryfikuje prawidłową identyfikację i ocenę czynników ryzyka oraz zarządzanie nimi w Państwa organizacji w trakcie formalizowania procesów, procedur i dokumentacji ochrony informacji;
- potwierdza troskę o ochronę informacji ze strony wyższego kierownictwa Państwa firmy;
- proces regularnych ocen pomaga w ciągłym monitorowaniu i poprawianiu wydajności.

CERTYFIKAT – NORMA PN-EN ISO 9001:2009 (ISO 9001:2008) – 800 punktów w rankingu ZPP

Systemy zarządzania jakością

Międzynarodowa Organizacja Normalizacyjna (ISO) opublikowała 15 listopada 2008 r. normę ISO 9001:2008 Quality management systems - Requirements, która zastępuje ISO 9001:2000.

ISO 9001:2008 nie zawiera nowych wymagań w porównaniu z normą z 2000 r. Wprowadzane zmiany mają na celu poprawę spójności wymagań normy i kompatybilności z ISO 14001:2004. Te postanowienia, które budziły wątpliwości i wymagały interpretacji, zapisano w sposób bardziej przejrzysty i jednoznaczny. Zmieniono sformułowania w tych miejscach, w których istniała możliwość błędnego tłumaczenia. Niektóre zagadnienia przedstawiono w bardziej logiczny i przejrzysty sposób, np. wymagania dotyczące nadzoru nad zapisami, auditów wewnętrznych, nadzoru nad wyrobem niezgodnym. W wielu punktach dodano uwagi ułatwiające zrozumienie lub wyjaśnienie wymagań, których dotyczą, np. procesów realizowanych na zewnątrz, nadzoru nad dokumentami, zasobów ludzkich, środowiska pracy, percepcji klienta co do tego, czy organizacja spełniła wymagania klienta.

ISO 9001:2008 jest podstawą do wdrożenia i certyfikacji Systemu Zarządzania Jakością (SZJ). Norma jest skonstruowana uniwersalnie. Nie zawiera wymagań dotyczących wyrobu (nie jest normą techniczną), tylko wymagania dotyczące systemu zarządzania. Wymagania te pozwalają na wdrożenie SZJ zarówno w przedsiębiorstwach produkcyjnych, usługowych, jak i w **administracji publicznej**.

Norma ISO 9001:2008 kieruje się zasadami:

- Koncentracja na kliencie - oznacza skupienie się na aktualnych oraz przyszłych potrzebach klienta oraz działania w celu ich zaspokojenia
- Przywództwo - oznacza, iż kadra kierownicza jest odpowiedzialna za wyznaczenie polityki, celów, strategii i kierunków rozwoju organizacji. Najwyższe kierownictwo odpowiada także za motywowanie i zaangażowanie wszystkich pracowników w rozwój organizacji i stworzenie korzystnych warunków do działania w tym kierunku.
- Zaangażowanie całej kadry - jedynie pełne zaangażowanie wszystkich pracowników w realizację strategii i celów organizacji pozwala na maksymalne wykorzystanie jej potencjału w celu uzyskania zamierzonych korzyści.
- Podejście procesowe - wszystkie działania organizacji traktować (zarządzać nimi) należy jako wzajemnie powiązane i oddziałujące między sobą procesy.
- Podejście systemowe do zarządzania - polega na zidentyfikowaniu, zrozumieniu i zarządzaniu wzajemnie powiązanymi procesami i traktowaniu ich jako system (zbiór wzajemnie powiązanych i oddziałujących elementów).
- Ciągłe doskonalenie - oznacza ciągłe, nieprzerwane, systematyczne działania w celu zwiększenia prawdopodobieństwa wzrostu zadowolenia klienta i innych stron. (audit wewnętrzny, działania korygujące i zapobiegawcze, itd.).
- Oparcie się na faktach - w procesie decyzyjnym należy opierać się na sprawdzonych i logicznie przeanalizowanych informacjach.
- Wzajemne korzystne powiązania z dostawcami - organizacja i jej dostawcy są zależni od siebie. Powiązania między nimi powinny być skonstruowane w ten sposób, aby przynosiły

obopólną korzyść. Powiązania te powinny pozwalać na szybkie reagowanie w wypadku szybko zmieniającej się sytuacji rynkowej oraz potrzeby klientów.



CERTYFIKAT ISO – NORMA ISO 14001:2004

Environmental management systems - Requirements with guidance for use

Podstawowym narzędziem realizacji zarządzania środowiskowego jest analiza cyklu życia produktu. Są to zorganizowane i ciągłe działania, których celem jest zapobieganie powstawaniu i systematyczna redukcja zanieczyszczeń.

Realizowany w przedsiębiorstwach program czystszej produkcji jest dobrym początkiem dla wdrożenia zarządzania środowiskowego według wymagań normy ISO 14001. System ten realizuje się między innymi w oparciu o Koło Deminga (metoda PDCA - planuj, wykonuj, sprawdzaj, działaj).

Istnieje kilka sposobów wdrażania systemu. Można opracować zintegrowany system dokumentacji w firmie. Zadanie to jest bardzo efektywne, ale jednocześnie prawie tak samo trudne. Można także zignorować istniejące dokumenty i zbudować oddzielną dokumentację ISO 14001. To z kolei spowoduje, że pracownicy będą mieć więcej niż jedną instrukcję działania. Trzeci sposób to dostosowanie dokumentacji do potrzeb zakładu. Ten sposób łączy część pierwszego i drugiego. Ostatni to komputerowa dokumentacja systemu.

Norma ISO 14001:2004 określa wymagania dotyczące systemu zarządzania środowiskowego w celu umożliwienia organizacji, opracowania i wdrożenia polityki oraz celów uwzględniających wymagania prawne i inne, które dotyczą organizacji, oraz informacje dotyczące znaczących aspektów środowiskowych. Norma dotyczy tych aspektów, które organizacja zidentyfikowała i które może nadzorować oraz tych, na które może mieć wpływ.

Norma ISO 14001:2004 ma zastosowanie do każdej organizacji, która pragnie ustanowić, wdrożyć, utrzymywać i doskonalić system zarządzania środowiskowego, mieć pewność co do postępowania zgodnego z ustaloną przez siebie polityką środowiskową i wykazać zgodność z normą przez samoocenę i własną deklarację lub dążenie do potwierdzenia zgodności przez strony zainteresowane organizacją, takie jak klienci lub dążenie do potwierdzenia własnej deklaracji przez zewnętrzne w stosunku do organizacji strony lub dążenie do certyfikacji/ rejestracji systemu zarządzania środowiskowego przez zewnętrzną organizację.

INTEGRACJA SYSTEMÓW

Zintegrowane systemy zarządzania

Istnienie kilku odrębnych systemów zarządzania w firmie jest irracjonalne i można to uznać za nienaturalny wytwór. Różne systemy zarządzania oczywiście mogą istnieć obok siebie. Dzieje się tak w przedsiębiorstwach, które upadły, upadną lub mają dużo szczęścia, że funkcjonują. Prawdłowo funkcjonujące przedsiębiorstwo musi kierować się spójnymi celami, spójną polityką. Czy ktoś podejmie się rozstrzygnąć spór w przedsiębiorstwie, gdzie istnieją dwie polityki - "co jest ważniejsze? jakość, czy środowisko?"

Zintegrowany system zarządzania, to system w którym spójnie funkcjonują co najmniej dwa podsystemy. Najczęściej, podstawą do budowy systemu zintegrowanego jest norma ISO 9001 oraz coraz bardziej popularne ISO 14001.

Wiele organizacji dostrzegło, że oprócz jakości, funkcjonują inne aspekty, które mogą pomóc osiągnąć sukcesu. Dbanie o środowisko, bezpieczeństwo pracy, bezpieczeństwo informacji, czy zarządzanie ryzykiem, daje nie tylko efekt marketingowy, ale i realne materialne korzyści dla organizacji. Wyżej wymienione aspekty znalazły swoje odzwierciedlenie w normach międzynarodowych. Na tych właśnie normach oparte są systemy zarządzania.

Racjonalnie funkcjonująca organizacja naturalnie dąży do tego, aby integrować system zarządzania. Organizacja z "dwoma systemami", to jak dwa mózgi rządzące jednym ciałem. Sposób integracji systemów zarządzania w dużej mierze zależy od sytuacji. Najczęściej spotykanym stanem jest ten, w którym firma ma wdrożony SZJ, zgodny z ISO 9001, a chce również funkcjonować zgodnie z ISO 14001. W takim wypadku na podbudowie funkcjonującego już systemu zarządzania jakością, buduje się zgodność z pozostałymi systemami. Dokonuje się tego poprzez rewizję polityki i celów organizacji oraz modyfikację dokumentacji.. Jest to sytuacja niezwykle komfortowa, gdyż normy te mają bardzo podobne podejście do kwestii systemów zarządzania i stosunkowo spójne wymagania.

Wszystkie wymagania normy ISO 14001:2004 można włączyć do dowolnego systemu zarządzania środowiskowego. Zakres zastosowania będzie zależał od takich czynników, jak polityka środowiskowa organizacji, charakter działań, wyrobów i usług oraz lokalizacji i warunków, w jakich organizacja działa.

SZKOLENIA WEWNĘTRZNE

Szkolenia dla pracowników Jednostek Samorządu Terytorialnego

Statystyka pokazuje, że tylko 20% - 30% incydentów wynika z powodów związanych ze stosowaniem technik informatycznych. Pozostała część jest efektem błędów ludzkich, braku szkoleń i niewłaściwym przygotowaniem pracowników do przeciwstawiania się nowym zagrożeniom.

Powszechne szkolenia pracownicze to znakomity sposób na podniesienie bezpieczeństwa w Jednostce. Pozwalają pracownikom łatwiej zapanować nad krytycznymi i ważnymi zasobami a także umożliwią poprawną realizację zadań. Polegają na wskazaniu każdemu pracownikowi mającemu dostęp do komputera obecnych zagrożeń jak i bezpiecznego poruszania się w Internecie.

W ramach naszej oferty, Amigable.pl proponuje Państwu nie tylko profesjonalne audyty i wdrożenia pozwalające na certyfikację w Związku Powiatów Polskich ale także doskonale zorganizowane, prowadzone na terenie Jednostki szkolenia pracownicze.

Związek Powiatów Polskich rekomenduje przeszkolenie wszystkich pracowników w Jednostkach Samorządu Terytorialnego w zakresie bezpieczeństwa przetwarzania informacji.

AGENDA SZKOLENIA PRACOWNIKÓW JST (czas trwania ok. 2 godzin)	
15 min	Legalność i licencje oprogramowania
15 min	Zarządzanie oprogramowaniem w JST
15 min	Zasady korzystania z sieci Internet
15 min	Bezpieczeństwo komputerów (polityka haseł, wygaszacze, monitory)
15 min	Czyste biurko i zakończenie pracy
15 min	Dane osobowe w JST i ich ochrona
15 min	Obowiązki przetwarzającego dane osobowe
15 min	Obowiązki Administratora Danych

Aby nie zakłócać ciągłości pracy Urzędu proponujemy podział pracowników na dwie lub więcej grup.

Po zakończeniu szkolenia każdy pracownik podpisuje dokument potwierdzający jego udział szkoleniu, który jest jednocześnie zobowiązaniem do przestrzegania zasad przedstawionych podczas szkolenia.

Urząd zobowiązany jest jedynie zapewnić odpowiednie warunki lokalowe do przeprowadzenia szkolenia.

SZKOLENIA ZEWNĘTRZNE

- **Wdrożenie Systemu Zarządzania Jakością wg PN-EN ISO 9001:2009 (ISO 9001:2008) w praktyce**

Szkolenie przygotowuje do samodzielnego wdrażania systemu zarządzania jakością wg normy PN-EN ISO 9001:2009 (ISO 9001:2008).

- **Auditor wewnętrzny / pełnomocnik Systemu Zarządzania Jakością wg normy ISO 9001:2008**

Szkolenie pozwala na zdobycie umiejętności i wiedzy niezbędnych w pełnieniu funkcji Pełnomocnika, jako osoby koordynującej wdrażanie i doskonalenie systemu jakości opartego na wymaganiach normy ISO 9001

- **Auditor wewnętrzny ISO 14001**

W ramach szkolenia uczestnicy poznają wymagania normy, ich interpretacje oraz sposoby realizacji. Poznają rolę i zadania funkcji pełnomocnika na etapie wdrożenia i utrzymywania systemu zarządzania. Omawiane są etapy i sposoby skutecznego wdrożenia systemu. Zajęcia prowadzone na bazie studium przypadku pozwalają samodzielnie prześledzić i przeanalizować przykładowe wdrożenie systemu.

Podczas warsztatów uczestnicy aktywnie przygotowują się do przeprowadzenia auditu, opracowują pytania audytowe, biorą udział w auditach szkoleniowych. Ćwiczą interpretację wymagań normy, identyfikację niezgodności, wyznaczanie działań korygujących i zapobiegawczych. Dodatkowo są prezentowane podstawy komunikacji niewerbalnej oraz elementy socjotechniki audytowej.

- **Auditor / Pełnomocnik Zintegrowanego Systemu Zarządzania wg. norm ISO 9001, 14001**

Szkolenie omawia szczegółowo wymagania norm ISO 9001, 14001, 18001. Ponadto przygotowuje do przeprowadzania auditów wewnętrznych i u dostawców, do prowadzenia prac związanych z wdrażaniem w organizacji Systemu Zarządzania oraz do pełnienia funkcji Pełnomocnika w organizacji posiadającej wdrożony system zarządzania.

- **Auditor / Pełnomocnik Systemu Zarządzania Bezpieczeństwem Informacji**

Szkolenie omawia szczegółowo wymagania normy ISO/IEC 27001:2005. Ponadto przygotowuje do przeprowadzania auditów wewnętrznych i u dostawców, do prowadzenia prac związanych z wdrażaniem w organizacji Systemu Zarządzania Bezpieczeństwem Informacji oraz do pełnienia funkcji Pełnomocnika w organizacji posiadającej wdrożony system zarządzania.