Regulamin prowadzenia przez Polski Komitet Normalizacyjny oceny Systemu Zarządzania Bezpieczeństwem Informacji na zgodność z wymaganiami normy PN-EN ISO/IEC 27001

Regulamin określa zasady współpracy, prawa i obowiązki oraz wzajemne zobowiązania stron, związane z procesem przeprowadzenia przez Polski Komitet Normalizacyjny auditu strony drugiej Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) na zgodność z wymaganiami normy PN-EN ISO/IEC 27001, wydaniem świadectwa stosowania SZBI oraz nadzoru nad systemem.

I. Terminologia.

Użyte w Regulaminie terminy oznaczają:

1. PKN – Polski Komitet Normalizacyjny.
2. Organizacja – podmiot, u którego na zasadach określonych w niniejszym Regulaminie PKN przeprowadza audit/audit nadzoru/audit ponownej oceny.
3. Audit – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z auditu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów auditu.
4. Audit strony drugiej – przeprowadzany przez strony zainteresowane organizacją wynikający z zawartych umów o współpracy.
5. Audit nadzoru – proces przeprowadzany przez PKN, w celu potwierdzenia zgodności Systemu z wymaganiami normy PN-EN ISO/IEC 27001, co najmniej raz na 12 miesięcy w okresie ważności świadectwa stosowania SZBI.
6. Audit ponownej oceny - proces przeprowadzany w celu odnowienia ważności świadectwa stosowania SZBI.
7. SZBI - System Zarządzania Bezpieczeństwem Informacji.
8. Autoryzacja – potwierdzenie, że dana osoba jest uprawniona do korzystania z systemu informacyjnego.
9. System informacyjny – system przetwarzania informacji wraz z zasobami (osobowymi, technicznymi, finansowymi).
10. Użytkownik – osoba korzystająca z systemu informacyjnego (pracownik Organizacji lub osoba autoryzowana przez Organizację).

II. Przeprowadzenie auditu

1. Warunkiem rozpoczęcia procesu jest:

1.1. złożenie przez Organizację wniosku o przeprowadzenie auditu,

1.2. podpisanie umowy na przeprowadzenie auditu oraz sprawowanie nadzoru nad Systemem.

2. Audit realizowany jest w 2 Etapach:

2.1. Etap 1 – analiza przekazanej przez Organizację dokumentacji Systemu pod kątem zgodności w wymaganiami normy PN-EN ISO/IEC 27001 oraz przygotowanie Planu Etapu 2,

2.2. Etap 2 auditu - badanie auditowe przeprowadzane przez PKN w siedzibie Organizacji (lub z siedziby PKN w formie zdalnej) w celu potwierdzenia zgodności zastosowanych zabezpieczeń z wymaganiami normy PN-EN ISO/IEC 27001. W uzgodnieniu z Organizacją auditowaną dopuszcza się przeprowadzenia auditów strony drugiej w formie zdalnej z siedziby PKN.

3. Termin przeprowadzenia auditu.

3.1. Etap 1 – nie później niż 14 dni od daty otrzymania kompletnej dokumentacji, o której mowa w pkt. 2.1,

3.2. Etap 2 – w terminie uzgodnionym przez strony, jednak nie później niż 21 dni od daty zakończenia Etapu 1., na podstawie Planu auditu udostępnionego Organizacji na co najmniej 7 dni od planowanego terminu badania auditowego.

4. W terminie 14 dni od przeprowadzenia Etapu 2 auditu PKN przekazuje Organizacji Raport z auditu.

4.1. w przypadku stwierdzenia niezgodności zostaną one przedstawione i opisane w Raporcie,

4.2. organizacja w terminie uzgodnionym przez strony podejmie działania korygujące i przedstawi PKN dowody potwierdzające usunięcie niezgodności,

4.3. w przypadku nieusunięcia przez Organizację niezgodności stosownie do zasad określonych w pkt. 4.2, PKN odmawia wydania świadectwa SZBI.

III. Świadectwo stosowania Systemu Zarządzania Bezpieczeństwem Informacji

1. Świadectwo jest przyznawane/odnawiane po spełnieniu następujących warunków:

1.1. niestwierdzenie w Raporcie z auditu/ Raporcie z auditu ponownej oceny niezgodności lub ich usunięcie stosowanie do zapisów Rozdziału II pkt 4.2,

1.2. uiszczenie przez Organizację opłaty za przeprowadzony audit/ audit ponownej oceny wg stawek naliczonych na zasadach określonych w Rozdziale VI,

2. Wydawane przez PKN świadectwo stosowania SZBI jest ważne przez 5 lat od daty jego przyznania, z zastrzeżeniem pkt. 3 i 6.

3. Świadectwo stosowania SZBI jest zawieszane w przypadku:

   3.1. stwierdzenia podczas auditu nadzoru niezgodności z kryteriami będącymi podstawą wydania świadectwa stosowania,

   3.2. nieprzeprowadzenia auditu nadzoru systemu raz na 12 miesięcy,

   3.3. nieuiszczenia opłaty z tytułu sprawowania nadzoru nad SZBI i wydanym świadectwem stosowania SZBI oraz przeprowadzenia auditu nadzoru.

4. O zawieszeniu świadectwa PKN informuje Organizację wzywając ją jednocześnie do podjęcia działań mających na celu usunięcie okoliczności uniemożliwiających utrzymanie ważności świadectwa.

5. Wezwanie, o którym mowa w pkt. 4 zawiera termin na usunięcie nieprawidłowości lub podjęcie działań umożliwiających wznowienie świadectwa SZBI.

6. Po bezskutecznym upływie terminu, o którym mowa w pkt. 5, PKN cofa świadectwo stosowania SZBI.

7. Świadectwo stosowania SZBI może być odnowione na kolejne 5 lat na wniosek Organizacji i po podpisaniu odrębnej umowy.

8. PKN przesyła Organizacji świadectwo stosowania SZBI w terminie 3 dni od spełnienia warunków określonych w pkt. 1.

IV. Audit nadzoru oraz sprawowanie nadzoru nad Systemem

1. W okresie ważności świadectwa stosowania SZBI PKN sprawuje nadzór nad Systemem SZBI.

   1.1. celem nadzoru jest sprawdzenie, czy SZBI jest skuteczny, rozważenie wpływu na SZBI ewentualnych zmian w działaniach Organizacji oraz potwierdzenie ciągłej zgodności z wymaganiami normy PN-EN ISO/IEC 27001.

   1.2. w ramach nadzoru PKN przeprowadza jeden audit nadzoru w każdym roku ważności świadectwa.

2. Audit nadzoru powinien odbyć się nie później niż 12 miesięcy od przyznania świadectwa stosowania SZBI lub auditu nadzoru.

3. PKN nie później niż 10 miesięcy od przyznania świadectwa stosowania SZBI lub auditu nadzoru przekazuje Organizacji informację o konieczności przeprowadzenia auditu nadzoru.

4. Audit nadzoru przeprowadzany jest na podstawie Planu auditu udostępnianego Organizacji na co najmniej 7 dni od planowanego terminu badania auditowego.

5. Do auditu nadzoru stosuje się postanowienia Rozdziału II pkt 4. – 4.3. odpowiednio.

V. Audit ponownej oceny

1. Wniosek o audit ponownej oceny musi być złożony nie później niż 3 miesiące przed upływem ważności świadectwa SZBI, z zastrzeżeniem, że proces odnowienia ważności świadectwa SZBI rozpoczyna się w momencie złożenia przez Organizację wniosku o przeprowadzenie auditu ponownej oceny.

2. Do auditu ponownej oceny mają zastosowanie postanowienia Rozdziału II odpowiednio.

VI. Należności finansowe za świadczone usługi i warunki płatności

1. Organizacja jest zobowiązana do regulowania wszelkich zobowiązań finansowych wynikających z umowy w terminie do 21 dni od dnia wystawienia faktur VAT, na rachunek bankowy PKN wskazany na tych fakturach.

2. Przerwanie auditu z przyczyn leżących po stronie Organizacji lub jego negatywny rezultat, skutkujące odpowiednio niewydaniem świadectwa SZBI lub jego cofnięciem – nie zwalniają Organizacji z zapłaty za zrealizowane przez PKN prace.

3. W przypadku, o którym mowa w pkt. 2 Organizacja zobowiązuje się do zwrotu wydatków poniesionych przez PKN w trakcie świadczenia usług związanych z realizacją niniejszej umowy obejmujących: koszty podróży, przejazdów i noclegów.

4. Koszt przeprowadzenia auditu jest obliczany wg następującego wzoru:

$$K_a = K_U\sqrt{L_L} + K_{SI} + K_Z$$

w którym:

K_a – koszt całkowity auditu

K_U – koszt wynikający z liczby użytkowników Systemów Informacyjnych auditowanej Organizacji:

K_U = 3 600 zł, jeżeli z Systemów Informacyjnych Organizacji korzysta do 100 użytkowników;

K_U = 4 800 zł, jeżeli z Systemów Informacyjnych Organizacji korzysta od 100 do 1000 użytkowników;

K_U = 6 000 zł, jeżeli z Systemów Informacyjnych Organizacji korzysta powyżej 1000 użytkowników;

L_L – liczba lokalizacji auditowanej Organizacji;

K_{SI} – koszt wynikający z liczby Systemów Informacyjnych auditowanej Organizacji:

K_{SI} = 1800 zł, jeżeli Organizacja posiada 1 System Informacyjny;

K_{SI} = 2400 zł, jeżeli Organizacja posiada od 2 do 5 Systemów Informacyjnych;

K_{SI} = 3000 zł, jeżeli Organizacja posiada powyżej 5 Systemów Informacyjnych;

K_Z – koszt wynikający z zastosowanych technik zabezpieczeń auditowanej Organizacji:

K_Z = 2000 zł, jeżeli Organizacja stosuje połączenia bez szyfrowania/podpisu cyfrowego;

K_Z = 2500 zł, jeżeli Organizacja stosuje połączenia z szyfrowaniem wbudowanym w standardowe wyposażenie i bez podpisu cyfrowego;

K_Z = 3000 zł, jeżeli Organizacja stosuje połączenia z szyfrowaniem/podpisem cyfrowym.

5. Koszt przeprowadzenia auditu nadzoru oraz sprawowania nadzoru nad SZBI stanowi 66% kwoty oszacowanej zgodnie z pkt. 4.

VII. Postanowienia końcowe

1. Strony zobowiązują się do takiego współdziałania w zakresie realizacji umowy, który zapewni najlepszy sposób jej wykonania.

2. Organizacja zobowiązana jest do:

2.1. utrzymania i doskonalenia swojego systemu zgodnie z wymaganiami normy PN-EN ISO/IEC 27001,

2.2. udzielania wszelkich informacji dotyczących systemu oraz dokumentacji, o której mowa w Rozdziale II pkt 2.1,

2.3. udostępnienia zasobów i wyposażenia niezbędnego dla pracy zespołu auditorów PKN oraz zapewnienia dostępu do wszystkich procesów, obszarów, zapisów i personelu w procesie auditu/auditu nadzoru/auditu ponownej oceny,

2.4. terminowego podejmowania działań korygujących i doskonalących,

2.5. bezzwłocznego powiadamiania PKN o dokonanych zmianach organizacyjno-prawnych, skutkujących zmianą w nadzorowanym systemie.

3. Organizacja ma prawo do:

3.1. powoływania się na świadectwo stosowania SZBI w działalności promocyjnej i reklamowej oraz w kontaktach ze swoimi klientami w odniesieniu do działalności objętej zakresem świadectwa stosowania SZBI.

3.2. składania skarg i odwołań związanych z pracą auditorów oraz procesem auditowania.

4. PKN zobowiązuje się, że przy wykonaniu przedmiotu zamówienia:

4.1. nie będzie zapoznawał się z dokumentami, analizami, zawartością dysków twardych i innych nośników informacji itp.- nie związanymi z prowadzonym auditem,

4.2. nie będzie udostępniał, rozpowszechniał i przekazywał w jakiejkolwiek formie informacji poufnych obejmujących nie ujawnione do wiadomości

publicznej informacje techniczne, technologiczne, handlowe lub organizacyjne Organizacji przekazane w jakiejkolwiek formie, które są oznaczone jako poufne lub tajemnicą przedsiębiorstwa,

4.3. nie będzie korzystał z żadnych informacji poufnych dla swojego własnego pożytku ani dla żadnych innych celów poza wykonaniem czynności związanych z auditem strony drugiej,

4.4. podejmie wszelkie uzasadnione środki celem zachowania poufności,

4.5. nie będzie informował osób trzecich o danych objętych nakazem poufności. Za osobę trzecią uważa się osoby nie wykonujące pracy lub usług na rzecz Organizacji,

4.6. zachowa w poufności przez czas nieoznaczony wszelkie informacje i dane uzyskane od Organizacji w związku z realizacją auditu strony drugiej i sprawowaniem nadzoru nad Systemem oraz nie będzie wykorzystywać tych informacji i danych do jakichkolwiek innych celów bez zgody Organizacji,

4.7. zobowiązanie do poufności nie będzie miało zastosowania w przypadkach, gdy na PKN z mocy prawa ciążyć będzie obowiązek udzielenia informacji objętej takim zobowiązaniem.