PROGRAM CERTYFIKACJI Systemów Zarządzania Bezpieczeństwem Informacji (ISMS)

Adresaci	**Dyrektor ds. Certyfikacji**	**Specjalista ds. Certyfikacji**
Otrzymują	+	oryginał
Egz. nr		

Opracował:	Maria Głowacka	Zatwierdził:	Tomasz Włodek
Data: 10.11.2023 r.	Podpis:	Data: 10.11.2023 r.	Podpis:

SPIS TREŚCI

1. POSTANOWIENIA OGÓLNE

Niniejszy program dotyczy certyfikacji systemu zarządzania bezpieczeństwem informacji zgodnego z normą PN-EN ISO/IEC 27001 „Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji - Wymagania". Program prezentuje zasady i procedury stosowane przez Zakład Certyfikacji w celu potwierdzenia zgodności systemu zarządzania bezpieczeństwem informacji organizacji wnioskodawcy z wymaganiami w/w normy.

Właścicielem programu jest Jednostka Certyfikująca „ZETOM" Katowice.

Celem Programu jest przedstawienie:

- procedury postępowania w procesie certyfikacji systemu zarządzania bezpieczeństwem informacji zgodnego z normą PN-EN ISO/IEC 27006
- zasad nadzoru nad wydanymi certyfikatami,
- procedury postępowania dot. skarg i odwołań zgłaszanych przez klientów,
- informacji dot. opłat za certyfikację,
- zasad stosowania znaku certyfikacji.

2. PRZEPISY PRAWNE I DOKUMENTY DOTYCZĄCE CERTYFIKACJI SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (ISMS) W RAMACH OCENY ZGODNOŚCI:

- PN-EN ISO/IEC 27001 „Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji - Wymagania",
- PN-EN ISO/IEC 27006 „Technika informatyczna. Techniki bezpieczeństwa. Wymagania dla jednostek prowadzących audyt i certyfikacją systemów zarządzania bezpieczeństwem informacji"
- IAF MD 1„Dokument obowiązkowy IAF dotyczący auditu i certyfikacji systemów zarzadzania zasad organizacji wielooddziałowych",
- IAF MD 2 „Dokument obowiązkowy IAF dotyczący przenoszenia akredytowanej certyfikacji systemów zarządzania"
- IAF MD 4 „Dokument obowiązkowy IAF dotyczący stosowania technologii informacyjno-komunikacyjnych („ICT") do celów prowadzenia auditów/ocen.
- IAF MD 5 „Dokument obowiązkowy IAF dotyczący ustalania czasu trwania auditów systemu zarządzania jakością i systemu zarządzania środowiskowego",
- IAF MD 11 „Dokument obowiązkowy IAF dotyczący zastosowania normy ISO / IEC 17021 w auditach zintegrowanych systemów zarządzania"
- DACS-01 „Akredytacja jednostek certyfikujących systemy zarządzania",

3. ZAKRES PROGRAMU CERTYFIKACJI ISMS

Zakres działalności Zakładu Certyfikacji w ramach certyfikacji systemu zarządzania bezpieczeństwem informacji prowadzony jest w określonych obszarach technicznych wg następujących branż:

Podział na obszary techniczne w systemie SZBI

Obszar techniczny	**Kod IAF**
Administracja publiczna	**36**
Działalność publiczna	8, 31, **34**, 37, **38**, **39**,
Usługi	30, **32**, **35**
Produkcja	1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, **33**

Pogrubienie i podkreślenie – obszar krytyczny
Obszary krytyczne:
32: Działalność finansowa i ubezpieczeniowa (PKD: 64, 65, 66)
33: Działalność związana z oprogramowaniem; Przetwarzanie danych, zarządzanie stronami internetowymi (PKD: 62, 63.1)
35: Działalność prawnicza, rachunkowo – księgowa i doradztwo podatkowe; Działalność ochroniarska w zakresie obsługi systemów bezpieczeństwa (PKD: 69, 80.2)
36: Administracja publiczna (PKD: 84)
38: Działalność szpitali; Praktyka lekarska (PKD: 86.1, 86.2)
39: Pozostała działalność usługowa w zakresie informacji (PKD: 63.9)

4. POUFNOŚĆ I BEZSTRONNOŚĆ

Zakład Certyfikacji zapewnia bezstronność, poufność i nie przekazywanie stronom trzecim informacji uzyskanych w trakcie procesu certyfikacji i nadzoru oraz innych źródeł za wyjątkiem przypadków przewidzianych prawem oraz gwarantuje ochronę praw własności.

Jeżeli przepisy prawne tak stanowią, to niezbędne informacje przekazywane są stosownym organom z kopią do Klienta.

Zakład Certyfikacji zapewnia, że wszystkie informacje (za wyjątkiem informacji publicznie udostępnionej przez klienta lub gdy uzgodniono to pomiędzy jednostką certyfikującą a klientem np. w celu odpowiadania na skargi) uzyskane lub wytworzone podczas realizacji działalności certyfikacyjnej traktowane są jako poufne. Zakład zapewnia, że przed ich upublicznieniem poinformuje klienta, o ile nie jest to zabronione przez prawo.

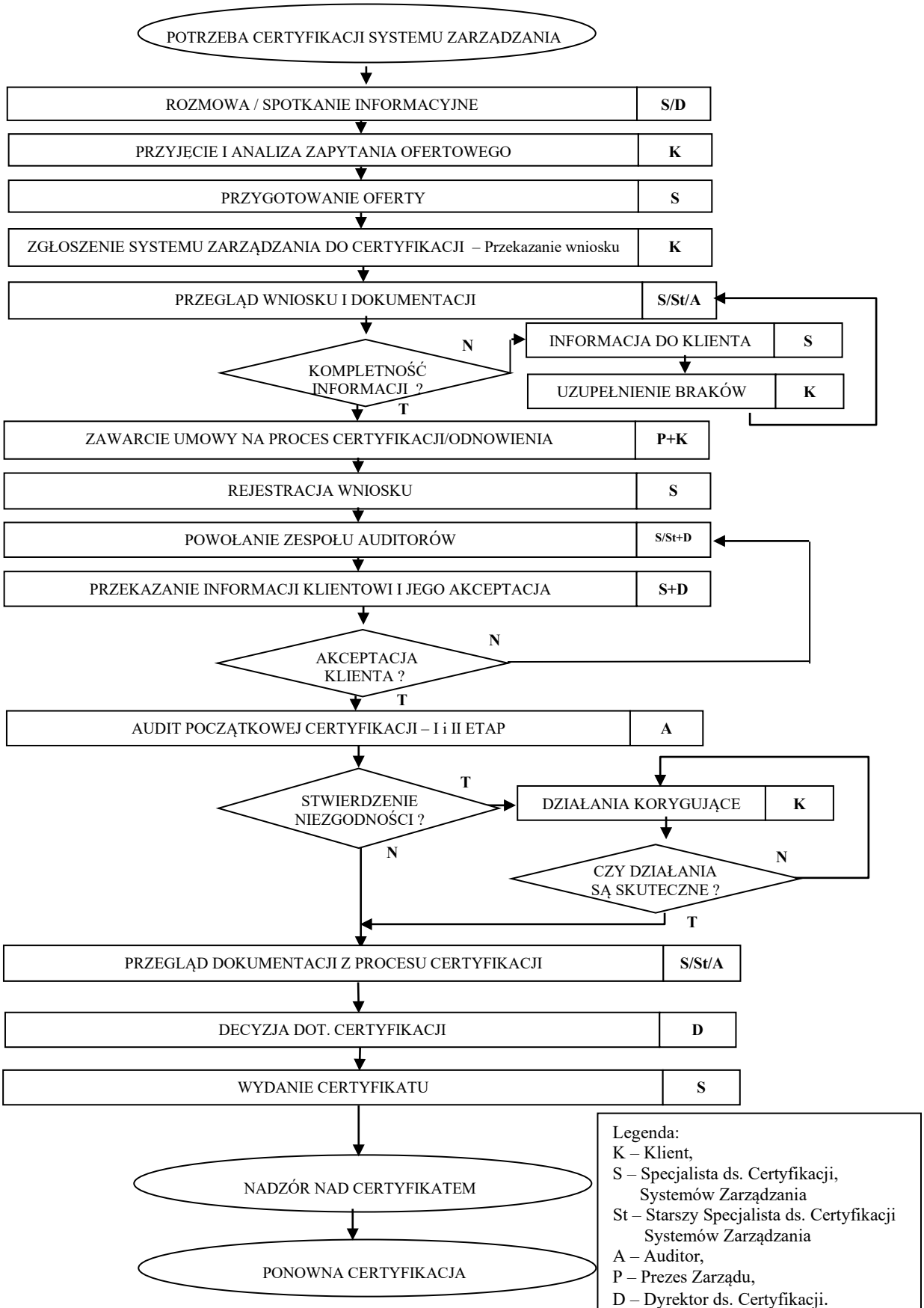
W strukturze Spółki „ZETOM" funkcjonuje Rada Jednostki Certyfikującej, która została powołana w celu zagwarantowania bezstronności prowadzonych działań certyfikacyjnych. Członkami Rady są przedstawiciele stron istotnie zainteresowanych działalnością certyfikacyjną.

5. SPOSÓB POSTĘPOWANIA

Proces Certyfikacji Systemu Zarządzania Bezpieczeństwem Informacji ISMS w Zakładzie Certyfikacji przebiega w następujący sposób (Rys. 1):

1. Zapytanie ofertowe
2. Oferta na proces certyfikacji systemu klienta,
3. Wniosek o przeprowadzenie procesu certyfikacji systemów zarządzania,
4. Przegląd wniosku
5. Zawarcie umowy na proces certyfikacji,
6. Przekazanie dokumentacji systemu zarządzania,
7. Powołanie zespołu auditującego oraz ustalenie czasu auditu,
8. Uzgodnienie terminu auditu,
9. Przygotowanie planu auditu,
10. Przeprowadzenie auditu początkowej certyfikacji (etap I, etap II) ,
11. Sporządzenie Raportu z auditu (etap I i etap II),
12. Decyzja o przyznaniu certyfikatu,
13. Rozliczenie kosztów i przekazanie Pisma – decyzji, raportu klientowi,
14. Wydanie certyfikatu,
15. Nadzór nad certyfikowanym systemem zarządzania (audit nadzoru),
16. Ponowna certyfikacja.

W wyniku przeprowadzonego procesu certyfikacji Zakład wydaje „Certyfikat Systemu Zarządzania Bezpieczeństwem Informacji”.



Rys. 1. Proces certyfikacji Systemu Zarządzania Bezpieczeństwem Informacji

5.1 INFORMACJE WSTĘPNE

Zakład Certyfikacji udziela wszystkich niezbędnych informacji zainteresowanemu na temat procesu certyfikacji systemu zarządzania bezpieczeństwem informacji, tj.:

- zakresu uprawnień jednostki certyfikującej system zarządzania bezpieczeństwem informacji,
- norm oraz przepisów prawnych związanych z certyfikacją systemu zarządzania,
- zasad certyfikacji systemu zarządzania bezpieczeństwem informacji,
- programu certyfikacji systemu zarządzania bezpieczeństwem informacji,
- dokumentu stanowiącego podstawę certyfikacji systemu zarządzania bezpieczeństwem informacji,
- dokumentacji wymaganej przy zgłaszaniu wniosku o certyfikację systemu zarządzania bezpieczeństwem informacji,
- kosztów związanych z certyfikacją systemu zarządzania bezpieczeństwem informacji,
- procedury odwołań i skarg.

Klient otrzymuje Program Certyfikacji w celu zapoznania się z zasadami i przebiegiem procesu certyfikacji systemu zarządzania bezpieczeństwem informacji oraz formularz zapytania ofertowego (Formularze stosowane w procesie certyfikacji dostępne są na stronie internetowej).

Specjalista ds. Certyfikacji na podstawie przekazanych informacji od klienta w „Zapytaniu ofertowym" sporządza ofertę certyfikacji systemu zarządzania która jest przekazywana klientowi wraz z formularzem „Wniosku o certyfikację systemu zarządzania". Oferta zawiera wstępną kalkulację kosztów procesu certyfikacji systemu zarządzania bezpieczeństwem informacji oraz szacunkowy czas auditu ustalony zgodnie z procedurą PSZ-09-02 „Ustalenie czasu auditu".

5.2 WNIOSEK O CERTYFIKACJĘ SYSTEMU ZARZĄDZANIA

Na wniosku o certyfikację systemu zarządzania podawany jest zakres certyfikacji objęty zgłoszonym systemem zarządzania bezpieczeństwem informacji zgodny z wymaganiami dokumentu odniesienia. Dopuszcza się zgłoszenie na jednym wniosku:

- większej liczby miejsc produkcji wyrobów, objętych tym samym systemem zarządzania,
- większej liczby systemów zarządzania.

Do wniosku dołączane są dokumenty określone przez Zakład Certyfikacji na odwrocie wniosku w p. II „Załączniki do wniosku" tj. dokumentacja systemu zarządzania, kserokopie certyfikatów systemu zarządzania, schemat organizacyjny przedsiębiorstwa, aktualny odpis właściwego rejestru sądowego lub ewidencji działalności gospodarczej, oraz wykaz wymagań prawnych obowiązujących Klienta w zakresie realizowanych wyrobów lub usług. Szczegółowy zakres dokumentacji dołączanej do wniosku każdorazowo uzgadniany jest z Wnioskodawcą.

Klient zobowiązany jest na dwa tygodnie przed ustalonym terminem I etapu auditu przekazać do Zakładu Certyfikacji dokumentację systemu zarządzania wraz z wykazem przekazywanych dokumentów.

Zakład Certyfikacji przyjmuje dokumentację w formie elektronicznej i/lub papierowej.

Dokumentacja przekazywana w formie elektronicznej powinna być zapisana i przekazana w sposób zapewniający bezpieczeństwo informacji.

5.3 PRZEGLĄD I REJESTRACJA WNIOSKU

Wniosek podlega przeglądowi pod względem formalnym, kompletności załączonej dokumentacji, oraz pod względem możliwości Zakładu do przeprowadzenia procesu certyfikacji zgłoszonego systemu zarządzania (np. zasobów Zakładu, kompetencji personelu).

Wnioskodawca jest pisemnie informowany o wpłynięciu wniosku, konieczności dokonania przedpłaty w formie zaliczki, ewentualnie o konieczności uzupełnienia dokumentów.

Wraz z pismem o zaliczkę przesyłana jest klientowi do zaakceptowania umowa o przeprowadzenie procesu certyfikacji. Umowa dotyczy wzajemnych praw i zobowiązań zainteresowanych stron w trakcie 3-letniego cyklu certyfikacji.

Po wpłaceniu zaliczki w wysokości określonej przez Zakład Certyfikacji, przesłaniu przez klienta podpisanej umowy, ewentualnych uzupełnień wniosku o brakujące dokumenty i po uzyskaniu pozytywnego wyniku przeglądu wniosek jest rejestrowany, a „Potwierdzenie przyjęcia wniosku(ów) o przeprowadzenie certyfikacji systemu zarządzania" jest przekazywane wnioskodawcy. Zarejestrowany wniosek jest podstawą do rozpoczęcia dalszych etapów procesu certyfikacji.

5.4 PRZYGOTOWANIE PROCESU OCENY I POWOŁANIE ZESPOŁU AUDITUJĄCEGO

Na podstawie analizy danych zawartych w zapytaniu ofertowym oraz wniosku Specjalista ds. Certyfikacji ustala optymalny czas auditu oraz dobiera skład zespołu auditującego odpowiednio do wnioskowanego zakresu certyfikacji. Czas auditu ustalany jest przez Specjalistę zgodnie z wymaganiami określonymi w Procedurze PSZ-09-02 „Ustalanie czasu auditu". Uzyskane wyniki zapisywane są w „Karcie ustalania czasu auditu".

Skład członków zespołu auditującego wybierany jest na podstawie wykazanych przez auditorów i zweryfikowanych przez ZETOM wymaganych kompetencji, które pozwalają na przeprowadzenie obiektywnego i skutecznego auditu. W uzgodnieniu z Wnioskodawcą do uczestnictwa w audicie dopuszcza się auditorów szkolących się / ewaluatorów, ekspertów technicznych, obserwatorów (członkowie organizacji klienta, konsultanci, personel jednostki akredytującej lub inne osoby).

Przed uruchomieniem auditu początkowej certyfikacji systemu zarządzania bezpieczeństwem informacji sporządzane są plan I etapu auditu początkowej certyfikacji, oraz program auditu obejmujący trzyletni cykl certyfikacji (tj. dwuetapowy audit początkowej certyfikacji, audit nadzoru w pierwszym i drugim roku oraz audit ponownej certyfikacji). Plan auditu przekazywany jest Wnioskodawcy w celu akceptacji lub zgłoszenia sprzeciwu wobec przedstawionej propozycji, nie później niż 7 dni od planowanego terminu auditu.

W przypadku braku akceptacji planu auditu Zakład wyznacza inny termin bądź inny skład zespołu.

W wyniku akceptacji zaproponowanego terminu i członków zespołu auditującego Specjalista ds. Certyfikacji przygotowuje zlecenie na przeprowadzenie auditu systemu zarządzania bezpieczeństwem informacji, które stanowi podstawę do wydania stosownych upoważnień i zobowiązań do poufności.

5.5 AUDIT POCZĄTKOWEJ CERTYFIKACJI

Proces certyfikacji systemu zarządzania bezpieczeństwem informacji rozpoczyna się od auditu początkowej certyfikacji (APC), który jest realizowany w dwóch etapach:

- ***I etap*** APC realizowany jest w celu:
  - sprawdzenia dokumentacji systemu zarządzania klienta,
  - oceny lokalizacji klienta,
  - przeprowadzenia rozmów z personelem klienta, aby określić gotowość do etapu II,
  - sprawdzenia statusu klienta,
  - zebrania informacji na temat zakresu systemu zarządzania, procesów oraz lokalizacji klienta,

- przeprowadzenia przeglądu przydziału zasobów do II-go etapu auditu,
- zaplanowania II-go etapu auditu poprzez zrozumienie systemu zarządzania klienta,
- oceny planowanych i realizowanych auditów wewnętrznych oraz przeglądów zarządzania.

Ustalenia z I Etapu auditu, ze wszystkimi stwierdzonymi zastrzeżeniami, dokumentowane są na formularzu „Notatki z auditu", a następnie komunikowane Klientowi na spotkaniu zamykającym.

Jeżeli w trakcie etapu I zostaną stwierdzone zastrzeżenia, które mogłyby być zakwalifikowane jako niezgodności podczas etapu II to auditor wiodący ustala z klientem termin rozwiązania zidentyfikowanych zastrzeżeń oraz sposób weryfikacji przez Zakład Certyfikacji podjętych przez Klienta działań.

- ***II etap*** APC realizowany jest w celu:
  - oceny wdrożenia i skuteczności systemu zarządzania,
  - sprawdzenia informacji i dowodów zgodności ze wszystkimi wymaganiami normy dotyczących zgłoszonego przez klienta systemu zarządzania,
  - wykonania pomiarów, monitorowania, raportowania i przeglądania kluczowych celów i zadań zgodnych z oczekiwaniami odpowiedniej normy lub innych dokumentów normatywnych,
  - sprawdzenia systemu zarządzania klienta oraz sposobu jego działania pod względem zgodności z prawem,
  - skontrolowania realizacji nadzoru operacyjnego klienta nad procesami, auditów wewnętrznych oraz przeglądów zarządzania,
  - potwierdzenia odpowiedzialności kierownictwa za politykę,
  - sprawdzenia powiązań pomiędzy wymaganiami normatywnymi, polityką, celami, odpowiedzialnością, kompetencjami personelu, procedurami, ustaleniami i wnioskami z auditów wewnętrznych.

Odstęp pomiędzy I a II etapem auditu ustalany jest indywidualnie w zależności od czasu potrzebnego na rozwiązanie przez klienta zidentyfikowanych podczas I-go etapu zastrzeżeń. Wyniki pierwszego etapu mogą doprowadzić do anulowania drugiego etapu.

Przegląd ustaleń z auditu oraz uzgodnienie wniosków z auditu dokonywane jest przez zespół auditujący po przeanalizowaniu wszystkich zebranych w trakcie auditu początkowej certyfikacji informacji i dowodów.

W oparciu o uzyskane podczas przeprowadzonego auditu dowody Auditor wiodący przygotowuje raport z auditu w dwóch egzemplarzach (jeden przeznaczony jest dla klienta, drugi dla Zakładu Certyfikacji) i przekazuje do Zakładu w terminie do 7 dni od spotkania zamykającego etap I oraz do 14 dni od spotkania zamykającego etap II.

Zastrzeżenia zapisywane są w raporcie z auditu, natomiast niezgodności są dokumentowane w Protokołach niezgodności, które stanowią załącznik do raportu. Weryfikacja skuteczności wprowadzonych korekcji lub działań korygujących następuje w wyniku przeglądu dostarczonej przez klienta dokumentacji i zapisów (dowody na realizację działań) lub w wyniku przeprowadzenia auditu dodatkowego. Warunkiem udzielenia certyfikacji, w przypadku wystąpienia dużej niezgodności, jest pozytywna ocena realizacji korekcji i/lub działań korygujących, natomiast w przypadku stwierdzenia małej niezgodności pozytywna ocena przedstawionego przez klienta planu dot. korekcji i działań korygujących.

5.6 PRZEGLĄD PRZED PODJĘCIEM DECYZJI

Działania zrealizowane podczas procesu certyfikacji oraz dokumentacja zgromadzona podczas procesu certyfikacji podlega przeglądowi w celu potwierdzenia zgodności systemu zarządzania bezpieczeństwem informacji z wymaganiami przyjętymi za podstawę certyfikacji. Przeglądu dokonuje kompetentny personel wyznaczony przez Specjalistę ds. Certyfikacji, nie związany z realizacją auditu i nie udzielający klientowi żadnych konsultacji dotyczących systemu zarządzania w okresie ostatnich 2 lat. Przeglądem objęte są raporty z auditu początkowej certyfikacji, raport z auditu nadzoru oraz inne dokumenty sporządzone w trakcie realizacji oceny (np. dokumenty potwierdzające realizację działań korygujących). Wyniki przeprowadzonego przeglądu są udokumentowane w Raporcie z przeglądu.

5.7 DECYZJA W SPRAWIE POCZĄTKOWEJ CERTYFIKACJI SYSTEMU ZARZĄDZANIA

Decyzja o wydaniu lub odmowie wydania certyfikatu podejmowana jest przez Dyrektora ds. Certyfikacji w oparciu o sporządzony Raportu z przeglądu oraz zawartą w raporcie z auditu rekomendację dot. decyzji w sprawie certyfikacji.

Certyfikat Systemu Zarządzania Bezpieczeństwem Informacji wydawany jest na okres 3 lat z datą ważności od dnia podjęcia decyzji o certyfikacji.

O wyniku podjętej decyzji związanej z przeprowadzonym procesem certyfikacji klient powiadamiany jest pisemnie. Klient wraz z decyzją otrzymuje fakturę oraz raport z auditu systemu zarządzania bezpieczeństwem informacji. Uregulowanie należności wg faktury jest podstawą do wysłania certyfikatu.

Informacja o udzielonej przez Zakład Certyfikacji zamieszczana jest w „Wykazie certyfikowanych klientów" dostępnym w jednostce na pisemne życzenie.

Wspomniany wykaz zawiera: nazwę klienta, dokument normatywny, zakres certyfikacji, lokalizację każdego certyfikowanego klienta, datę ważności certyfikatu.

5.8 ODMOWA WYDANIA CERTYFIKATU

W przypadku nie przyznania certyfikatu klient otrzymuje pisemną decyzję wraz z uzasadnieniem oraz fakturę za wykonane czynności.

Klient jest informowany o możliwości odwołania się od decyzji Dyrektora ds. Certyfikacji w terminie 14 dni od jej doręczenia do Rady Jednostki Certyfikującej. Tryb rozpatrywania odwołania przebiega zgodnie z Procedurą PSZ-09-07 „Odwołania i skargi".

5.9 NADZÓR NAD CERTYFIKATEM

Zakład Certyfikacji sprawuje nadzór nad wydanym certyfikatem tj. ocenia spełnienie wymagań stawianych podczas początkowej certyfikacji przez system zarządzania klienta. W trakcie 3-letniego cyklu certyfikacji systemu zarządzania realizowane są 2 audity nadzoru. Pierwszy audit nadzoru przeprowadzany jest nie później niż 12 miesięcy od dnia podjęcia decyzji o certyfikacji. Odstęp między kolejnymi auditami planowanymi nie przekracza 12 miesięcy.
W formie pisemnej / elektronicznej o terminie każdego auditu klient jest informowany z wyprzedzeniem.

Nadzór nad wydanymi certyfikatami realizowany jest poprzez:

- planowane audity nadzoru (AN),
- audity specjalne – audity nieplanowane,
- audity dodatkowe (pełne lub ograniczone) – prowadzone w celu weryfikacji skuteczności korekcji i działań korygujących,

- przegląd oświadczeń klienta dot. jego działalności (np. materiały promocyjne, strona internetowa),
- przegląd dokumentów i zapisów dostarczonych przez klienta (w wersji papierowej lub elektronicznej),

5.9.1 Planowany audit nadzoru

Planowany audit nadzoru przeprowadzany jest zgodnie z programem auditów, z częstotliwością określoną w umowie (co najmniej 1 raz w roku) i obejmuje:

- ocenę realizacji auditów wewnętrznych i przeglądu zarządzania,
- przegląd działań podjętych w celu wyeliminowania zidentyfikowanych niezgodności podczas poprzedniego auditu,
- sprawdzenie sposobu postępowania ze zgłoszonymi skargami / reklamacjami,
- ocenę skuteczności systemu zarządzania ze względu na realizację celów organizacji klienta,
- sprawdzenie postępu planowanej działalności nastawionej na ciągłe doskonalenie,
- ciągły nadzór operacyjny,
- przegląd wszelkich zmian zaistniałych w organizacji,
- sprawdzenie sposobu stosowania znaków i/lub powoływania się na certyfikację.

5.9.2 Prowadzenie auditów z zastosowaniem technologii informacyjno-komunikacyjnych

Audity systemów zarządzania mogą być przeprowadzane metodą zdalną z wykorzystaniem technologii informacyjno-komunikacyjnej (ICT).
Metoda auditów zdalnych z wykorzystaniem technologii ICT może być stosowana jedynie dla realizacji auditów nadzoru oraz jedynie w jednej z dwóch następujących sytuacji:

- losowa sytuacja nadzwyczajna, niezależna od Klienta, która uniemożliwia zespołowi auditowemu przeprowadzenia czynności auditowych bezpośrednio w organizacji Klienta. Do sytuacji takich zalicza się: klęski żywiołowe, epidemię, pandemię, sytuację polityczną, działania wojenne, terroryzm,
- występują oddziały zamiejscowe organizacji Klienta, objęte zakresem certyfikowanego systemu zarządzania, w których realizowane są procesy i działania, co do których, na podstawie analizy ryzyka, określono możliwość auditu zdalnego.

Przeprowadzenie auditu zdalnego każdorazowo musi zostać poprzedzone udokumentowanymi uzgodnieniami z Klientem, których wynikiem jest pisemna zgoda Klienta na realizację auditu w przedmiotowej formie.

5.9.3 Audity specjalne

Audity specjalne – audity mogą zostać przeprowadzone:

- w ramach rozszerzenia zakresu certyfikatu,
- w przypadku zgłoszenia do jednostki uzasadnionych skarg,
- w przypadku wprowadzenia przez klienta znaczących zmian w systemie zarządzania, w procesie produkcji lub w wyrobie,
- w ramach postępowania dotyczącego wznowienia wcześniej zawieszonego certyfikatu,
- w wyniku przeniesienia certyfikacji,
- w ramach potwierdzenia przez jednostkę (jeśli konieczne) wdrożenia działań korygujących dotyczących niezgodności stwierdzonych podczas auditów planowanych.

Audity specjalne przeprowadza się (za wyjątkiem auditów specjalnych w ramach rozszerzenia zakresu certyfikacji) jako audity z krótkim terminem powiadamiania lub bez zawiadomienia.

Podstawą do uruchomienia auditu nadzoru jest zlecenie na przeprowadzenie auditu, który realizowany jest w uzgodnionym terminie przez zaakceptowany przez posiadacza certyfikatu zespół auditujący.

5.10 WYKORZYSTANIE CERTYFIKATU I ZNAKÓW CERTYFIKACJI PRZEZ KLIENTA

Organizacja ma prawo powoływać się na uzyskany certyfikat w prowadzonej działalności reklamowej i w kontaktach z klientami w odniesieniu do działalności objętej zakresem certyfikatu.

Zasady posługiwania się znakiem certyfikacyjnym przedstawione są w Załączniku nr 2 „Wzór znaku „ZETOM – ISO 27001" dot. certyfikacji systemu zarządzania bezpieczeństwem informacji oraz zasady posługiwania się tym znakiem".

Sposób wykorzystania certyfikatu oraz znaków certyfikacji podlega ocenie podczas auditów nadzoru i ponownej certyfikacji.

Podstawą oceny sposobu wykorzystywania certyfikatów jest:
- sprawdzenie posługiwania się certyfikatem i znakiem jednostki certyfikującej w materiałach reklamowych i promocyjnych, na drukach firmowych itp.,
- analiza reklamacji zgłoszonych organizacji i/lub wpływających do Zakładu Certyfikacji oraz zapisów z działań korygujących podjętych przez certyfikowaną organizację w związku z reklamacjami,
- ocena skuteczności działań podejmowanych przez certyfikowaną organizację w związku z reklamacjami.

5.11 DECYZJE PODEJMOWANE W RAMACH NADZORU NAD CERTYFIKATEM

Na podstawie wniosków z przeprowadzonego auditu, raportu z auditu, raportu oceny, ewentualnych niezgodności i podjętych korekcji bądź działań korygujących jednostka certyfikująca może podjąć następujące decyzje:
- utrzymanie certyfikacji,
- przedłużenie certyfikacji,
- rozszerzenie zakresu certyfikacji,
- zawieszenie certyfikacji,
- przywrócenie ważności certyfikatu,
- cofnięcie zakresu certyfikacji,
- ograniczenie zakresu certyfikacji,
- przeniesienie praw do certyfikatu.

5.11.1 Utrzymanie certyfikacji

Jednostka certyfikująca może utrzymywać certyfikację systemu zarządzania bezpieczeństwem informacji organizacji klienta jeżeli spełnione są następujące warunki:
- pozytywne wyniki auditu systemu zarządzania bezpieczeństwem informacji – brak dużych niezgodności,
- pozytywna ocena w zakresie wykorzystywania przez auditowanego dokumentów certyfikacyjnych, znaków lub raportów z auditów (dot. nadzoru i ponownej certyfikacji),
- wywiązywanie się przez klienta z zobowiązań finansowych wobec „ZETOM" Katowice,
- pozytywne wyniki przeglądu sporządzonego raportu. Przegląd realizowany jest przez personel niezwiązany z procesem auditowania w przypadku pojawienia się jakiejkolwiek niezgodności lub innej sytuacji, która mogłaby prowadzić do zawieszenia lub cofnięcia certyfikacji.

Jeżeli warunki utrzymania certyfikatu nie zostaną spełnione, Zakład Certyfikacji może zawiesić, cofnąć lub ograniczyć zakres certyfikacji.

5.11.2 Przedłużenie ważności certyfikatu

Przedłużenie okresu ważności certyfikacji systemu zarządzania bezpieczeństwem informacji następuje na wniosek posiadacza certyfikatu na podstawie auditu ponownej certyfikacji przeprowadzonej w ostatnim roku ważności certyfikatu.

Decyzja w sprawie przedłużenia certyfikacji podejmowana jest na podstawie wyników auditu ponownej certyfikacji, przeglądu systemu w okresie certyfikacji oraz na podstawie skarg otrzymanych od zainteresowanych stron.

Proces przedłużenia ważności certyfikacji realizowany jest zgodnie z Procedurą PSZ-09-05 „Ponowna certyfikacja”.

5.11.3 Rozszerzenie zakresu certyfikatu

Rozszerzenie zakresu certyfikatu może obejmować obszary działań systemu zarządzania bezpieczeństwem informacji, które nie były objęte certyfikatem w ramach tego samego dokumentu odniesienia oraz nowe miejsca działalności klienta objęte certyfikatem.
Rozszerzenie następuje na podstawie wniosku zgłoszonego przez posiadacza certyfikatu.
Działania mające na celu ocenę spełnienia wymagań w nowych obszarach działań lub nowych lokalizacjach mogą obejmować:

- przeprowadzenie auditu specjalnego,
- przegląd i analizę dokumentacji i zapisów klienta.

Certyfikat uwzględniający nowe obszary lub nowe lokalizacje wydawany jest na postawie wyników auditu specjalnego oraz na podstawie wyników dotychczasowych działań w ramach sprawowanego nadzoru.

5.11.4 Zawieszanie zakresu certyfikacji

Zawieszenie certyfikatu następuje w przypadku:

- zgłoszenia przez klienta czasowej rezygnacji z certyfikacji,
- stwierdzenia w trakcie auditu nadzoru lub auditu ponownej certyfikacji niezgodności w działaniu certyfikowanego systemu zarządzania z wymaganiami, które stanowią podstawę certyfikacji,
- braku zadeklarowania przez klienta usunięcia stwierdzonych przyczyn obniżonej skuteczności działania systemu zarządzania,
- niedotrzymywania przez klienta warunków umowy certyfikacyjnej,
- braku możliwości przeprowadzenia auditu nadzoru lub auditu ponownej certyfikacji z wymaganą częstotliwością z winy klienta,
- nieprawidłowego wykorzystywania dokumentów certyfikacyjnych, znaków certyfikacji,
- niedostosowania się do ustaleń wynikających ze zmiany wymagań „ZETOM” w określonym terminie,
- powstania innych uzasadnionych sytuacji (np. brak realizacji działań korygujących, nieuregulowanie zobowiązań finansowych itp.),
- stwierdzenia że system zarządzania klienta stale lub w poważnym stopniu nie spełnia wymagań certyfikacyjnych,
- nie zgłoszenia przez organizację zakończenia działalności w którymkolwiek z oddziałów przed planowanym auditem nadzoru (w przypadku organizacji wielooddziałowej).

W przypadku podjęcia decyzji o zawieszeniu certyfikatu, klient jest pisemnie powiadamiany o warunkach, po których spełnieniu certyfikat zostanie przywrócony. Certyfikat może być zawieszony maksymalnie na 6 miesięcy. Zawieszenie certyfikatu jest jednoznaczne

z zaprzestaniem powoływania się na certyfikację przez klienta do momentu jej przywrócenia przez „ZETOM".

5.11.5 Ograniczanie zakresu certyfikacji

Ograniczenie zakresu certyfikatu następuje w przypadku:
- stwierdzenia niespełnienia wymagań certyfikacyjnych dla pewnych części zakresu certyfikacji,
- na wniosek posiadacza certyfikatu,
- w celu wykluczenia części, które nie spełniają wymagań,
- nie spełnienia przez klienta wymagań certyfikacyjnych w poważnym stopniu bądź stale.

Ograniczenie zakresu certyfikatu następuje poprzez wydanie nowego certyfikatu o ograniczonym zakresie, zachowując ten sam numer certyfikatu i termin ważności.

5.11.6 Cofnięcie zakresu certyfikacji

Cofnięcie certyfikatu następuje w przypadku:
- stwierdzenia nieskuteczności systemu zarządzania, powodującego konieczność wprowadzenia zasadniczych zmian w systemie,
- niewłaściwego powoływania się na certyfikację i/lub wprowadzające w błąd wykorzystywanie certyfikatów i znaków certyfikacji,
- nie spełnienia w ustalonym terminie warunków postawionych przy zawieszeniu certyfikatu,
- nie wywiązywania się klienta z zobowiązań finansowych wobec „ZETOM" Katowice,
- na wniosek posiadacza certyfikatu,
- powoływania się na certyfikat po jego zawieszeniu,
- zaprzestania prowadzenia działalności objętej zakresem certyfikacji,
- niedostosowania się do ustaleń wynikających ze zmiany wymagań „ZETOM" Katowice w określonym terminie,
- niedotrzymania warunków umowy,
- wydania nowego certyfikatu w wyniku przeniesienia praw własności, zmiany dokumentu normatywnego, zmiany nazwy posiadacza certyfikatu,
- likwidacji firmy (likwidacji spółki, ogłoszenie jej upadłości obejmującej likwidację majątku dłużnika).

O cofnięciu certyfikacji posiadacz certyfikatu jest niezwłocznie pisemnie powiadamiany.

Zawieszenie lub cofnięcie certyfikatu systemu zarządzania pociąga za sobą ten sam skutek dla wszystkich aneksów wydanych do tego certyfikatu, a także zobowiązuje klienta do zaprzestania powoływania się na certyfikację we wszelkich materiałach reklamowych.

W pismach zawierających w/w decyzje umieszczana jest informacja o prawie do odwołania od decyzji.

Proces zawieszania, ograniczenia i cofania certyfikacji i realizowany jest zgodnie z Procedurą PSZ-09-06 „Zawieszanie, cofanie lub ograniczanie zakresu certyfikacji".

5.12 AUDIT PONOWNEJ CERTYFIKACJI – RECERTYFIKUJĄCY

Ponowna certyfikacja następuje na podstawie złożonego przez klienta wniosku, a zaplanowana jest na **3 miesiące** przed upływem ważności certyfikacji. Do wniosku należy dołączyć aktualną dokumentację wraz z informacjami dotyczącymi zmian w organizacji i w dokumentacji wprowadzonymi po poprzednim audicie.

W trakcie auditu ponownej certyfikacji należy dokonać:

- oceny stałego spełniania wszystkich wymagań dokumentów odniesienia dotyczących systemu zarządzania,
- potwierdzenia stałej zgodności i skuteczności systemu zarządzania,
- sprawdzenia / weryfikacji funkcjonowania systemu zarządzania i raportów w okresie objętym certyfikacją.

W sytuacjach gdy nastąpiły znaczące zmiany w systemie zarządzania (np. zmiany legislacyjne) dopuszcza się przeprowadzenie pierwszego etapu auditu (jeśli konieczne).

W przypadku stwierdzenia na audicie ponownej certyfikacji dużych niezgodności jednostka certyfikująca określa granice czasowe dla korekcji i działań korygujących. Działania te powinny być wdrożone i zweryfikowane przed upływem ważności certyfikacji. Podstawą do udzielenia ponownej certyfikacji jest pozytywna ocena działań dot. ponownej certyfikacji. Data wydania nowego certyfikatu jest datą podjęcia decyzji w sprawie ponownej certyfikacji.

5.13 PRZENOSZENIE AKREDYTOWANEJ CERTYFIKACJI SYSTEMU ZARZĄDZANIA

Przeniesienie certyfikacji następuje wtedy gdy klient certyfikowany przez inną jednostkę certyfikującą postanawia zostać klientem Jednostki Certyfikującej „ZETOM" Katowice Sp. z o.o.

Do przeniesienia kwalifikowane mogą być jedynie certyfikacje akredytowane przez sygnatariusza IAF MLA. Organizacje, których certyfikacje nie są objęte taką akredytacją traktowane są jak nowi klienci.

Certyfikowane i posiadające akredytację systemy zarządzania mogą być przejęte przez Jednostkę Certyfikującą ZETOM na każdym etapie cyklu certyfikacyjnego i skutkują wydaniem certyfikatu Jednostki Certyfikującej „ZETOM" Sp. z o.o. ważnego do końca pozostałego jeszcze cyklu certyfikacyjnego.

Certyfikaty zawieszone i wycofane lub takie, w których stwierdzono duże niezgodności nie mogą podlegać procesowi przeniesienia i należy je traktować jak nowe certyfikacje wymagające dwuetapowego auditu całego systemu zarządzania.
Przebieg postępowania jest zgodny z dokumentem obowiązkowym IAF dotyczącym przenoszenia akredytowanej certyfikacji systemów zarządzania IAF MD 2.

Zasady przeniesienia certyfikowanej akredytacji określa Procedura PSZ-09-11 „Przeniesienie certyfikacji akredytowanej".

5.14 PRZENIESIENIE PRAW DO CERTYFIKACJI ORAZ DOKONYWANIE ZMIAN W CERTYFIKACIE

Przeniesienie praw do certyfikacji następuje na wniosek posiadacza certyfikatu i może mieć miejsce w przypadku:

- zmiany nazwy i/lub adresu organizacji dla której wydano certyfikat,
- zmiany statusu prawnego lub stosunków własnościowych organizacji, dla których wydano certyfikat.

Do wniosku klient dołącza dokument potwierdzający zmianę statusu prawnego certyfikowanej organizacji (np. KRS, Księga Rejestrowa). Po przeanalizowaniu przez Zakład Certyfikacji dokumentów podejmowana jest decyzja o przeniesieniu praw certyfikacji. Decyzję taką podejmuje Dyrektor ds. Certyfikacji. W przypadku, gdy zmianie ulega tylko forma prawna danej firmy lub dokonywana jest zmiana nazwy firmy, przeniesienie praw może nastąpić bez konieczności przeprowadzania auditu dodatkowego. W przypadku, gdy zmianie ulega np. lokalizacja lub Zarząd, decyzja o przeniesieniu praw certyfikowanej organizacji podejmowana jest po przeprowadzeniu auditu dodatkowego.

Zasady przeniesienia praw do certyfikatu oraz dokumentację niezbędną do w tym zakresie określa Procedura PSZ-09-12 „Przeniesienie praw do certyfikatu".

5.15 CERTYFIKACJA ORGANIZACJI WIELOODDZIAŁOWYCH

Jednostka Certyfikująca ZETOM Katowice prowadzi certyfikację systemów zarządzania organizacji mających sieć oddziałów w celu zapewnienia, że audit daje wystarczające zaufanie co do zgodności systemu zarządzania z normą oraz PN-ISO/IEC 27001 we wszystkich zgłoszonych oddziałach.

Audit certyfikacyjny oraz kolejne audity w nadzorze i audity ponownej oceny są przeprowadzane zgodnie z wymaganiami określonymi w Dokumencie obowiązkowym IAF MD 1 dotyczącym zasad auditu i certyfikacji organizacji wielooddziałowych. Organizacja wielooddziałowa nie musi być jedną osobą prawną, lecz wszystkie oddziały powinny mieć prawne lub kontraktowe powiązanie z funkcją centralną organizacji oraz powinny być objęte pojedynczym systemem zarządzania, ustanowionym, wprowadzonym i poddanym stałemu nadzorowi i auditom wewnętrznym przez funkcję centralną.

Funkcja centrala powinna być auditowana podczas każdej certyfikacji i ponownej oceny oraz co najmniej raz w roku w nadzorze.

Zasady prowadzenia auditu w organizacjach wielooddziałowych określa Procedura PSZ-09-03 „Auditowanie organizacji wielooddziałowych".

5.16 ODWOŁANIA I SKARGI

Prawo do odwołania od decyzji jednostki certyfikującej oraz wniesienia skargi mają wszyscy klienci na każdym etapie procesu certyfikacji. Ponadto prawo do wniesienia skargi mają wszystkie strony zainteresowane (m.in. organy władzy państwowej, organizacje pozarządowe, konsumenci i inni członkowie społeczeństwa). Odwołania i skargi przyjmowane są w formie pisemnej. Kierowane są do Rady Jednostki Certyfikującej.

Odwołanie od decyzji powinno być złożone w terminie 14 dni od jej doręczenia. Warunkiem odwołania jest uregulowanie wszystkich zobowiązań finansowych wynikających z wykonywanych przez „ZETOM" czynności związanych z certyfikacją systemu zarządzania bezpieczeństwem informacji lub nadzorem. Skarga może dotyczyć sposobu przeprowadzania procesu certyfikacji. O sposobie załatwienia odwołania / skargi klient jest powiadamiany pisemnie wraz z uzasadnieniem podjętej decyzji.

Ewentualne sprawy sporne natury formalno-prawnej mogące zaistnieć przy realizacji procesu mogą być rozstrzygane wg prawa polskiego przez właściwe sądy.

Tryb załatwiania skarg i odwołań reguluje Procedura PSZ-09-07 „Odwołania i skargi". Procedura udostępniana jest na życzenie klienta

5.17 OPŁATY

Opłaty związane z kosztami certyfikacji systemu zarządzania bezpieczeństwem informacji (wydaniem / rozszerzeniem zakresu Certyfikatu) oraz kosztami nadzoru w okresie ważności Certyfikatu (utrzymanie, przeniesienie certyfikacji) pokrywa Zleceniodawca / Posiadacz Certyfikatu.

Koszty nalicza się zgodnie z procedurą finansową Spółki nr PSZ-09-09 na podstawie Cennika obowiązującego w dniu zakończenia czynności, których opłata dotyczy.

Cennik Opłat ustalony jest przez „ZETOM" w oparciu o opinie Rady Jednostki Certyfikującej.

Cennik Opłat przekazywany jest na życzenie klienta.

6. ZAŁĄCZNIKI

- Załącznik nr 1 – Tabela czasu pracy auditorów systemu zarządzania bezpieczeństwem informacji.

- Załącznik nr 2 – Wzór znaku „ZETOM – ISO 27001” dot. certyfikacji systemu zarządzania bezpieczeństwem informacji oraz zasady posługiwania się tym znakiem.

7. KARTA ZMIAN

Data	Strona	Punkt	Zakres zmian	Wprowadzający zmianę	Zatwierdzający

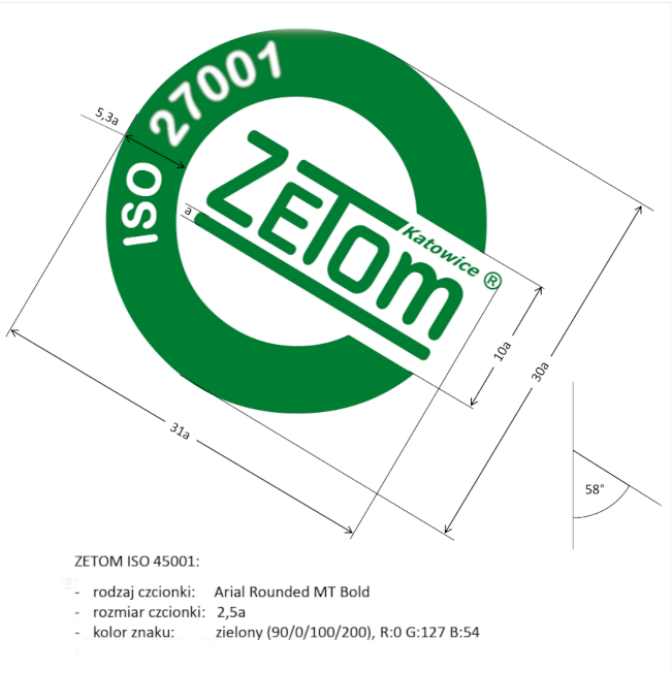
Załącznik nr 1
do ISMS

Tabela czasu pracy Auditorów podczas oceny w procesie certyfikacji systemu zarządzania bezpieczeństwem pracy.

LP	Efektywna liczba personelu	Czas auditu Etap 1 + Etap 2 (liczba dni)	Efektywna liczba personelu	Czas auditu Etap 1 + Etap 2 (liczba dni)
1	1 ÷ 5	5	626 ÷ 875	17,5
2	6 ÷ 10	5	876 ÷ 1175	18,5
3	11 ÷ 15	6	1176 ÷ 1550	19,5
4	16 ÷ 25	7	1551 ÷ 2025	21
5	26 ÷ 45	8,5	2026 ÷ 2675	22
6	46 ÷ 65	10	2676 ÷ 3450	23
7	66 ÷ 85	11	3451 ÷ 4350	24
8	86 ÷ 125	12	4351 ÷ 5450	25
9	126 ÷ 175	13	5451 ÷ 6800	26
10	176 ÷ 275	14	6801 ÷ 8500	27
11	276 ÷ 425	15	8501 ÷ 10700	28
12	426 ÷ 625	6,5	> 10700	Zgodnie z powyższą progresją

Załącznik nr 2
do ISMS

Wzór znaku „ZETOM – ISO 27001”
dot. certyfikacji systemu zarządzania bezpieczeństwem informacji oraz zasady posługiwania się tym znakiem



1. Zatwierdzony przez Prezesa Zarządu Zakładów Badań i Atestacji „ZETOM” im. Prof. F. Stauba w Katowicach sp. z o.o. wzór znaku **„ZETOM – ISO 27001”** stanowi graficzny wyróżnik certyfikowanego systemu zarządzania bezpieczeństwem informacji przez niezależną jednostkę „ZETOM” Katowice.

   Znak powinien być stosowany bez zmian formy graficznej.
   Dopuszcza się powiększenie lub pomniejszenie znaku oraz stosowanie przy jego odtwarzaniu kolorystyki PANTONE DE 280-1C – C = 90, M = 0, Y = 100, K = 20 lub R = 0, G = 127, B = 54, lub jako czarno-białe.
2. Użytkownikami znaku są Posiadacze Certyfikatu Systemu Zarządzania Bezpieczeństwem Informacji objętego umową, w okresie jego ważności.
3. Znak może być stosowany przez Posiadacza Certyfikatu Systemu Zarządzania Bezpieczeństwa Informacji na drukach firmowych, dokumentach i materiałach handlowych, promocyjnych oraz reklamowych, itp. z jednoznacznym wskazaniem, że odnosi się do systemu zarządzania objętego zakresem certyfikatu.
4. Znak nie może być używany w sposób, który mógłby oznaczać lub sugerować, że odnosi do działalności, która jest poza zakresem certyfikacji.
5. Znak nie może być używany na wyrobie, opakowaniu wyrobu widocznym dla konsumenta, ani w dowolny inny sposób (np. na etykietach), który mógłby być interpretowany jako oznaczający zgodność wyrobu. Dopuszcza się stosowanie oświadczenia na opakowaniu wyrobu lub towarzyszącej informacji, że klient posiada certyfikowany system zarządzania. Oświadczenie powinno zawierać odniesienie do:

- identyfikacji klienta (nazwa producenta wyrobu),
- rodzaj systemu zarządzania (np. bezpieczeństwo informacji) i mającej zastosowanie normy,
- jednostki certyfikującej wydającej certyfikat.

6. Znak nie może być używany w sposób wprowadzający w błąd lub naruszający reputację jednostki certyfikującej oraz w sposób, który narażałby „ZETOM" Katowice na utratę publicznej wiarygodności.

7. Znak nie może być stosowany na sprawozdaniach z badań laboratoryjnych, świadectwach wzorcowania lub sprawozdaniach z inspekcji.

8. W przypadku utraty ważności Certyfikatu lub jego zawieszenia, Posiadacz zobowiązany jest do natychmiastowego zaprzestania stosowania znaków **„ZETOM – ISO 27001"**

9. Posiadacz nie może przenosić prawa do posługiwania się znakiem **„ZETOM – ISO 27001**" na inne podmioty (np. podwykonawców).

10. W przypadku nadużycia lub fałszerstwa znaku **„ZETOM – ISO 27001**" jednostka certyfikująca „ZETOM" Katowice może cofnąć lub zawiesić ważność Certyfikatu oraz zastrzega sobie możliwość dochodzenia swoich praw z wykorzystaniem wszystkich dostępnych prawnie środków

11. Sposób stosowania znaku będzie podlegał kontroli w ramach nadzoru nad wydanym Certyfikatem Systemu Zarządzania Bezpieczeństwa Informacji.

12. Warunkiem stosowania znaku jest wywiązywanie się z określonych w umowie zobowiązań wobec jednostki certyfikującej.