Śląska Sieć
Metropolitalna
Sp. z o.o.

SSM.ZSZ.POL.01

Polityka Bezpieczeństwa Informacji i Ciągłości Działania

Zintegrowany System Zarządzania

Spis treści

I. DEKLARACJA NAJWYŻSZEGO KIEROWNICTWA.

1. Nadrzędnym celem Śląskiej Sieci Metropolitalnej Spółki z ograniczoną odpowiedzialnością z siedzibą w Gliwicach jest zapewnienie niezakłóconego świadczenia wysokiej jakości usług oraz bezpieczeństwa przetwarzanych informacji.

2. Dla osiągnięcia założonego celu strategicznego Spółka dokłada wszelkiej staranności w utrzymaniu wysokiego standardu realizacji usług oraz ciągłości działania Procesów Krytycznych poprzez zapewnienie odporności Spółki na incydenty ciągłości działania.

3. W trosce o najwyższą jakość świadczonych usług, Spółka nieustannie podnosi standardy bezpieczeństwa informacji przetwarzanych w ramach działalności prowadzonej na rzecz klientów i partnerów Spółki, a także informacji wytworzonej w organizacji w związku z prowadzoną działalnością statutową.

4. Informacja podlega nadzorowi i ochronie, zgodnie z przepisami prawa i regulacjami wewnętrznymi, adekwatnie do wagi informacji oraz zidentyfikowanych zagrożeń.

5. Realizacja celów Polityki bezpieczeństwa informacji i ciągłości działania gwarantuje klientom i partnerom Spółki, nieprzerwaną i profesjonalną współpracę, rzetelną realizację zawartych umów i porozumień oraz zadań wynikających z innych instrumentów prawnych, w szczególności bezpieczeństwo powierzonych lub udostępnionych informacji.

6. W celu zapewnienia najwyższych standardów bezpieczeństwa informacji i ciągłości działania, przy jednoczesnym uwzględnieniu specyfiki organizacji oraz wymagań prawnych, Spółka wdrożyła Zintegrowany System Zarządzania **(ZSZ)**, zgodny z wymaganiami norm:

   1) PN-EN ISO/IEC 27001:2023-08 „Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności - Systemy zarządzania bezpieczeństwem informacji – Wymagania", oraz

   2) PN-EN ISO 22301:2020-04 – „Bezpieczeństwo i odporność - System zarządzania ciągłością działania - Wymagania".

7. Zakres ZSZ obejmuje wszystkie lokalizacje Spółki, realizowane procesy i informacje będące własnością Spółki oraz powierzone do przetwarzania lub udostępnione przez klientów i partnerów Spółki.

8. Głównymi celami wdrożonego ZSZ jest:

   1) zapewnienie przetwarzania informacji w sposób gwarantujący ich dostępność, poufność i integralność,
   2) utrzymania działalności na poziomie umożliwiającym realizację Procesów Krytycznych,
   3) minimalizację prawdopodobieństwa i negatywnych skutków wystąpienia zakłóceń w działaniu Procesów Krytycznych, oraz

4) przygotowanie do podjęcia adekwatnych reakcji w przypadku wystąpienia incydentu ciągłości działania, poprzez osiągnięcie odpowiedniego poziomu organizacyjnego i technicznego.

9. Dla osiągnięcia celów ZSZ Zarząd Spółki zapewnia:

1) określenie zasad postępowania z informacją oraz zakłóceniem działalności;

2) zintegrowanie wymagań bezpieczeństwa informacji i ciągłości działania z procesami funkcjonującymi w Spółce,

3) dbałość o osiąganie zamierzonych wyników funkcjonowania bezpieczeństwa informacji i ciągłości działania,

4) wspieranie pracowników, stażystów i praktykantów oraz innych osób wykonujących pracę przyczyniających się do osiągnięcia skuteczności bezpieczeństwa informacji i ciągłości działania oraz dostarczanie im niezbędnych zasobów,

5) monitorowanie działania Procesów Krytycznych Spółki, celem wczesnej identyfikacji zdarzeń zakłócających ciągłość działania oraz zminimalizowanie ich wpływu na funkcjonowanie,

6) gotowość do podejmowania adekwatnych działań w sytuacjach awaryjnych i kryzysowych,

7) przydzielenie odpowiedzialności za informację i jej bezpieczeństwo,

8) identyfikację ryzyk bezpieczeństwa informacji aktywów oraz utraty ciągłości działania Procesów Krytycznych, ich analizę i ewaluację oraz podejmowanie adekwatnych działań minimalizujących poziom ryzyka, zapewniając zainteresowanym stronom, że ryzyka są odpowiednio zarządzane,

9) stosowanie adekwatnych zabezpieczeń organizacyjnych, osobowych, fizycznych i technologicznych,

10) monitorowanie, aktualizowanie, dostosowywanie rozwiązań systemowych do zmieniających się przepisów prawa powszechnie obowiązującego oraz standardów odniesienia,

11) stosowanie uznanych międzynarodowych standardów oraz najlepszych praktyk z zakresu bezpieczeństwa informacji, bezpieczeństwa teleinformatycznego oraz zarządzania ciągłością działania,

12) uwzględnianie zasad bezpieczeństwa informacji już na etapie projektowania procesów, systemów informacyjnych i zabezpieczeń,

13) podnoszenie wiedzy i świadomości pracowników,

14) promowanie wśród pracowników ciągłego doskonalenia przydatności, adekwatności i skuteczności ZSZ,

15) prowadzenie działalności w zgodzie z wymogami prawa, regulacjami wewnętrznymi, zawartymi umowami i porozumieniami bądź wynikającymi z innymi instrumentów prawnych.

10. Zarząd Spółki zobowiązuje się do wspierania utrzymania i doskonalenia ZSZ, zgodnego z wymaganiami norm wskazanymi w ust. 6 powyżej, poprzez nadzorowanie, promowanie, monitorowanie, regularne przeglądy oraz wspieranie wszelkich inicjatyw podejmowanych w celu ochrony działalności i informacji, a także zapewnienie niezbędnych zasobów finansowo - organizacyjnych dla zapewnienia skuteczności i efektywności ZSZ.

11. Wszyscy pracownicy Spółki, stażyści i praktykanci, a także inne osoby wykonujące prace na rzecz Spółki są zobowiązani do znajomości i przestrzegania wymagań ZSZ oraz dbałości o jego rozwój i skuteczność wdrażanych rozwiązań. Kontrahenci zobowiązani są do stosowania adekwatnych zasad i reguł bezpieczeństwa informacji i ciągłości działania, odpowiednio do ram prowadzonej współpracy.