I. Cel i zakres

Celem Systemu Zarządzania Bezpieczeństwem Informacji jest zapewnienie, iż informacje uznane za ważne z punktu widzenia Organizacji, w tym dane osobowe, są poufne, integralne oraz dostępne.

Zakresem systemu zarządzania bezpieczeństwem informacji objęte są dane uznane przez Organizację za ważne lub wrażliwe, przetwarzane w ramach działalności związanej ze świadczeniem usług doradztwa prawnego i technicznego w tym sporządzanie opinii przez biegłego sądowego w zakresie ochrony środowiska

Realizacja powyższych zadań odbywa się w Kancelarii Ekologicznej Sp. z o.o., zlokalizowanej w Poznaniu przy ulicy Cedrowej 11/7. Działalność Kancelarii ma zasięg ogólnokrajowy.

Z zakresu systemu zostało wyłączone wymaganie zawarte w Załączniku A do normy ISO/IEC 27001, które zostały uwzględnione w dokumencie Deklaracja stosowania.

II. Definicje

Poufność - pewność, że informacja jest użytkowana przez wszystkich, którzy powinni mieć do niej dostęp oraz chroniona przed dostępem wszystkich, którzy nie powinni wejść w jej posiadanie;

Integralność - pewność, że informacja nie została zniekształcona lub zmodyfikowana przez niepowołane osoby;

Dostępność - pewność, że informacja jest dostępna zawsze wtedy kiedy jest potrzebna dla osób, które powinny mieć do niej dostęp.

Wymagania prawne – obejmują zapisy aktów prawa w zakresie ochrony danych osobowych:
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie przepływu takich danych;
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
- Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

III. Deklaracja Zarządu

Najwyższe Kierownictwo Kancelarii Ekologicznej Sp. z o.o. wdraża System Bezpieczeństwa Informacji zgodny z wymaganiami Normy ISO/IEC 27001 dla zapewnienia, iż wszystkie przetwarzane w Firmie dane i informacje objęte statusem chronionych, są bezpieczne.

Bezpieczeństwo informacji przetwarzanych w Organizacji jest zapewnione, poprzez podejście oparte na trzech podstawowych kryteriach przetwarzania danych, rozumianych jako:
- Poufność;
- Integralność;
- Dostępność.

Powyższe cele są realizowane poprzez:

- wyznaczenie osób odpowiedzialnych za koordynacje działań związanych z zarządzaniem bezpieczeństwem informacji,
- określenie zasad przetwarzania informacji oraz obszarów, w których może się ono odbywać,
- podnoszenie świadomości i kwalifikacji w zakresie zarządzaniem bezpieczeństwem informacji wśród pracowników Organizacji,
- ciągłe doskonalenie systemu zapewnia bezpieczeństwa informacji funkcjonującego w Organizacji zgodnie z wymaganiami normy ISO/IEC 27001.

Niniejsza Polityka Bezpieczeństwa Informacji jest rozpowszechniania wśród wszystkich pracowników, a cele w niej zawarte są zrozumiałe i realizowane na wszystkich szczeblach organizacyjnych.

IV. Podstawowe zasady w zakresie zarządzania bezpieczeństwem informacji

1. Cały Personel Organizacji, stosownie do swoich obowiązków i zajmowanych stanowisk, jest odpowiedzialny za przestrzeganie zasad niniejszej Polityki Bezpieczeństwa Informacji, co potwierdza własnoręcznym podpisem.

2. Pracownicy, którzy mają dostęp do danych osobowych oraz informacji niejawnych powinni być dopuszczeni do nich na zasadach określonych w obowiązujących wymaganiach prawnych.

3. Ochrona informacji bazuje na kontroli dostępu do danych i ich przetwarzanych. W odniesieniu do informacji sklasyfikowanych jako chronione w Organizacji obowiązuje zasada „wiedzy uzasadnionej", zgodnie z którą dostęp do tej kategorii informacji powinien być uzasadniony realizacją powierzonych zadań. W przypadku braku takiego uzasadnienia, odmawia się dostępu do w/w danych.

4. Wszystkie osoby pracujące w Organizacji mające dostęp do informacji chronionych muszą być okresowo szkolone z zasad ochrony informacji.

5. Osoby nie będące pracownikami Organizacji składają pisemne zobowiązania (oświadczenie) o zachowaniu poufności informacji chronionych, z którymi zapoznali się w związku z wykonywaniem pracy dla Organizacji.

6. Podmioty zewnętrzne świadczące usługi na rzecz Organizacji podpisują umowę o zachowaniu w poufności informacji chronionych, które zostały im przekazane lub udostępnione w związku z realizacją określonych usług na rzecz Organizacji.

7. Pomieszczenia, w których przetwarzane będą informacje chronione powinny być zabezpieczone przed nieautoryzowanym dostępem, wpływami środowiska itp.

8. Urządzenia, na których są przetwarzane i przechowywane informacje chronione powinny być zabezpieczone przed niepowołanym dostępem, kradzieżą, wpływami środowiska itp.

V. Odpowiedzialność

Właściciel organizacji (wchodzi w skład zespołu ds. Bezpieczeństwa Informacji)
Odpowiedzialny jest za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji. Prezes decyduje o współpracy w zakresie bezpieczeństwa z innymi podmiotami, a także może wyrazić zgodę na udostępnienie stronom trzecim informacji stanowiących tajemnicę firmy.

Pełnomocnik ds. Zintegrowanego Systemu Zarzadzania (wchodzi w skład zespołu ds. Bezpieczeństwa Informacji) odpowiada za:

- kontrolę dokumentów Zintegrowanego Systemu Zarzadzania,
- opracowywanie nowych i aktualizację podstawowych dokumentów Zintegrowanego Systemu Zarzadzania,
- zapewnienie, że dokumenty są zawsze czytelne i oznaczone w odpowiedni sposób,
- rozpowszechnianie dokumentów Zintegrowanego Systemu Zarzadzania wśród pracowników,
- wycofywanie i przechowywanie dokumentów nieaktualnych, zapobiegając niezamierzonemu stosowaniu nieaktualnych dokumentów,
- wdrożenie i koordynowanie zapewniania bezpieczeństwa informacji oraz związanych z nim polityk i procedur,
- szkolenie pracowników w zakresie Zintegrowanego Systemu Zarzadzania, w tym Systemu Zarządzania Bezpieczeństwem Informacji.

Pracownicy odpowiedzialni są za:

- przetwarzanie danych w zakresie swoich kompetencji,
- prawidłowy obieg dokumentów zgodnie z zakresem obowiązków,
- przestrzeganie wdrożonych zasad funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji,
- przetwarzanie i zarządzanie danymi oraz informacjami w sposób zgodny z wdrożonym Systemem Zarządzania Bezpieczeństwem Informacji.

Ponadto: **odpowiedzialność za bezpieczeństwo informacji w Organizacji ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków**.

Zespół ds. Bezpieczeństwa Informacji odpowiedzialny jest:

- dokonywanie przeglądu i zatwierdzanie polityki bezpieczeństwa informacji oraz ogólnego podziału odpowiedzialności,
- uzgadnianie określonych metodyk i procesów związanych z bezpieczeństwem informacji, np. szacowanie ryzyka, system klasyfikacji dla potrzeb bezpieczeństwa,
- monitorowanie istotnych zmian narażenia aktywów informacyjnych na podstawowe zagrożenia,
- dokonywanie przeglądu i monitorowanie naruszeń bezpieczeństwa informacji,
- zatwierdzanie ważniejszych przedsięwzięć zmierzających do podniesienia poziomu bezpieczeństwa informacji.

Spotkania Zespołu ds. Bezpieczeństwa Informacji odbywają się w ramach przeglądów zarządzania oraz wraz z pojawiającymi się potrzebami, za zgodą Właściciela.

VI. Komunikacja

Zasady komunikowania informacji w Organizacji i poza nią opisuje procedura Zintegrowanego Systemu Zarządzania – *P-13 Komunikacja*.

Organizacja komunikuje na zewnątrz tylko informacje, których komunikację umożliwiają wymagania prawne. Szczegółowe zasady SZBI oraz informacje powierzone przez klientów nie są komunikowane na zewnątrz. Mogą być udostępnione na bezpośrednie zapytanie zainteresowanych stron.

VII. Ciągłe doskonalenie

Organizacja stale doskonali swój system poprzez analizowanie wyników audytów wewnętrznych, wyników analizy ryzyka, pomiaru skuteczności zabezpieczeń i przeglądu zarządzania. Na podstawie tych elementów podejmowane są plany i działania mające pozytywnie wpłynąć na bezpieczeństwo informacji.

Zgodnie z obowiązującą procedurą *P-04 Działania doskonalące, korygujące i zapobiegawcze* prowadzony jest rejestr wszelkich działań istotnych dla funkcjonowania Zintegrowanego Systemu Zarządzania i podejmowane są na bieżąco kroki mające na celu doskonalenie systemu.

VIII. Zasoby

Organizacja zapewnia zasoby niezbędne do realizacji celów SZBI. Zasoby podlegają ewidencji w *Wykazie aktywów.*

IX. Współpraca z podmiotami zewnętrznymi

Każda osoba trzecia, która narusza sferę bezpieczeństwa nie zostaje pozostawiona bez nadzoru personelu firmy. Dostęp do powierzchni biurowych wszelkiego personelu technicznego zajmującego się konserwacją sprzętu, ochrony, partnerów handlowych i innych osób jest nadzorowany przez pracowników Organizacji.

Zasady współpracy firmy z innymi Organizacjami oparta są na stosownych umowach. Zawierając te umowy firma ma zawsze na względzie, aby obejmowały one deklarację o zachowanie poufności informacji.

Wymiana informacji o zagrożeniach w zakresie bezpieczeństwa osób i mienia oraz zakłócenia spokoju i porządku publicznego następuje poprzez:

- Udzielanie wzajemnej pomocy w realizacji zadań ochrony, zapobieganiu przestępczości.
- Udzielanie wyczerpujących informacji o zagrożeniu dla bezpieczeństwa i porządku publicznego,

- Współdziałanie w zabezpieczeniu powstałych awarii.

Współdziałanie przy zabezpieczeniu miejsc popełnienia przestępstw i wykroczeń w granicach chronionych obiektów realizowane jest poprzez:

- Zabezpieczenie śladów na miejscu zdarzenia,
- Ustalenie świadków zdarzenia, a także wykonywanie innych czynności, jakie zleci Policja,
- Niedopuszczenie osób postronnych na miejsce przestępstwa, wykroczenia.

Zabezpieczenie mienia organizacji na wypadek pożaru lub awarii:

- Działania podejmuje się zgodnie z procedurą *P-09 Gotowość reagowania na awarie*.
- Dla każdej zidentyfikowanej sytuacji awaryjnej przyjęto plan ciągłości działania, z którym pracownicy i właściciele Organizacji są zapoznani i zobowiązali się do ich stosowania.

X. Zarządzanie Informacją

Firma uważnie zarządza swoimi aktywami informacyjnymi w celu zapewnienia im wymaganego poziomu bezpieczeństwa.

Organizacja oszacowuje ważność poszczególnych aktywów informacyjnych oraz określa szczegółowe zasady postępowania z danymi grupami informacji oraz grupy pracowników posiadające do nich dostęp.

Na podstawie oszacowania potencjalnych strat wynikających z incydentów związanych z naruszeniem lub przechwyceniem każdej informacji uważanej w organizacji za wrażliwą, przeprowadzana jest okresowa analiza ryzyka i opracowywany jest plan postępowania z ryzykiem. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów Organizacji.

Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla aktywów o ryzykach większych niż ustalony poziom ryzyka akceptowalnego. Ryzyka są przeglądane na przeglądach zarządzania oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

XI. Autoryzacja nowych urządzeń

Każde nowe lub zmienione urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek inny sposób wpływać na bezpieczeństwo informacji musi zostać zweryfikowane na zgodność z wymaganiami systemu bezpieczeństwa informacji i zaakceptowane przez wskazaną osobę. W zależności od miejsca wprowadzenia zmian za dopuszczenie do użytkowania nowych urządzeń odpowiada Kierownik lub Pełnomocnik ds. ZSZ. Szczegółowe wymagania w zakresie autoryzacji nowych urządzeń znajdują się w Księdze Procedur SZBI.

XII. Zasoby ludzkie, kompetencje, szkolenia, świadomość

Organizacja dba o to, by Pracownicy włączeni w realizację poszczególnych procesów byli kompetentni, w celu zminimalizowania ryzyka wystąpienia błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów.

Zarząd podejmuje wraz z Pełnomocnikiem ds. ZSZ działania mające na celu podnoszenie świadomości dotyczącej bezpieczeństwa informacji wśród pracowników. Działania te polegają na bezpośrednim przekazywaniu informacji o zmianach w systemie zarządzania bezpieczeństwem informacji oraz na okresowym przeprowadzaniu szkoleń w zakresie SZBI.

Szczegółowe wymagania w zakresie zarządzania zasobami ludzkimi znajdują się w Księdze Procedur SZBI.

XIII. Bezpieczeństwo fizyczne i środowiskowe

Organizacja zapewnia wysoki poziom bezpieczeństwa informacji poprzez ograniczenie dostępu do wrażliwych informacji osobom postronnym, a także zabezpieczenie informacji przed utratą integralności lub dostępności na skutek uszkodzenia lub zniszczenia nośnika, czy też miejsca przechowywania informacji.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z wyznaczeniem stref bezpieczeństwa, zasadami pracy oraz administrowaniem prawami dostępu do nich.

Szczegółowe wymagania w zakresie bezpieczeństwa fizycznego i środowiskowego zawarto w Księdze Procedur SZBI.

XIV. Zarządzanie systemem komputerowym i siecią

Firma dba o przestrzeganie zasad związanych z utrzymywaniem i użytkowaniem systemów informatycznych i sieci w celu zapewnienia poufności, integralności i dostępności przetwarzanej przez nie informacji własnych.

Skuteczna realizacja postawionego celu możliwa jest dzięki:

- kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistyczną firmą zapewniającą obsługę techniczną całego systemu informatycznego,
- kontrolowaniu wprowadzania wszelkich zmian do infrastruktury technicznej,
- nadzorowaniu usług dostarczanych przez osoby trzecie,
- wdrożeniu zabezpieczeń chroniących przed oprogramowaniem złośliwym,
- usystematyzowanemu tworzeniu i testowaniu kopii bezpieczeństwa,
- przestrzeganiu opracowanych zasad postępowania z nośnikami,
- bieżącym monitorowaniu aktywów informacyjnych, w tym informatycznych, pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów.

- monitorowaniu poziomu incydentów w systemach informatycznych i mechanizmom reagowania w przypadkach ich wystąpienia.

XV. Kontrola dostępu do informacji wrażliwych

Organizacja kontroluje dostęp do informacji uznanych przez nią za ważne lub wrażliwe, poprzez zarządzanie dostępem do tych informacji. Organizacja zapewnia, że dostęp do informacji, miejsc, urządzeń lub systemów ich przetwarzania mają tylko osoby uprawnione.

Pomieszczenia biurowe w firmie oddzielone są od bezpośredniego dostępu osób postronnych oraz istnieje możliwość zamykania ich na klucz. Wstęp osób postronnych na teren Organizacji możliwy jest tylko w obecności przedstawiciela Organizacji (pracownika, pełnomocnika ds. ZSZ, prezesa, zarządu).

Dostęp do systemu zawierającego kluczowe dla Organizacji dane, maja tylko upoważnieni pracownicy, po uprzednim zalogowaniu się na indywidualne konto.

Szczegółowe wymagania w zakresie dostępu do informacji wrażliwych zawarto w Księdze Procedur SZBI.

XVI. Udzielanie informacji stronom trzecim

Każda informacja udostępniana stronom trzecim (zewnętrznym) podlega ochronie. Przed udostępnieniem/wymianą informacji każdy pracownik jest odpowiedzialny za upewnienie się, że może taką informację przekazać zainteresowanej stronie. W przypadku wątpliwości o przekazaniu informacji decyduje właściwy przełożony.

Udostępnianie informacji na zewnątrz obywa się zgodnie z procedurą *P-13 Komunikacja.*

XVII. Zarządzanie incydentami

W przypadku wszelkich incydentów w Organizacji powiadamiany jest Pełnomocnik ds. SZBI. Z jego udziałem dokonywana jest wstępna analiza incydentu, po czym podejmowane są działania zgodne z zasadami reakcji na zdarzenia. Po wystąpieniu incydentu natychmiast podejmowane są działania mające na celu usunięcie ewentualnych skutków zaistnienia incydentu, a następnie wszystkie incydenty są szczegółowo analizowane i podejmowane są dalsze decyzje właściwe dla danej sytuacji.

Incydenty są rejestrowane i analizowane przez członków Zespołu Bezpieczeństwa.

XVIII. Polityka stosowanie zabezpieczeń kryptograficznych

Podstawa prawna:

Opracowanie przez Kancelarii Ekologicznej Sp. z o.o. założeń w zakresie polityki kryptograficznej jest związane z koniecznością zapewnienia jak najwyższych standardów dla ochrony informacji niejawnych i środków ochrony kryptograficznej, które powinny być stosowane w urządzeniach i narzędziach

kryptograficznych przeznaczonych do ochrony informacji niejawnych, a także w urządzeniach lub narzędziach służących do realizacji zabezpieczenia teleinformatycznego przeznaczonego do ochrony informacji niejawnych.

Technologia kryptograficzna używana jest w 3 aspektach:

1. Zabezpieczanie danych znajdujących się na komputerach, autoryzacja z wykorzystaniem użytkownika i hasła lub klucza kryptograficznego.
2. Zabezpieczane połączeń zdalnych do infrastruktury Jednostki z wykorzystaniem kanałów cyfrowanych VPN.
3. Bezpieczne logowania poprzez sieć internetową do usług administrowanych przez firmy trzecie – dostęp https i protokół TSL i SSL, poczta elektroniczna.

Należy stosować następujące sposoby kryptograficznej ochrony danych:

- Przy przesyłaniu danych za pomocą poczty elektronicznej stosuje się protokoły szyfrowane – wykorzystując szyfrowane połączenia (TLS lub SSL), metodę RSA i certyfikaty S/MIME,
- W przypadku korespondencji z organami administracji publicznej stosowane są podpisy elektroniczne, certyfikowane podpisy osobiste oraz narzędzia ich weryfikacji.
- W przypadku korespondencji za pośrednictwem ePUAP– Wszystkie dane systemu są chronione przez zaawansowane zabezpieczenie programowe i sprzętowe, a podczas przesyłania pomiędzy użytkownikiem i ePUAP są szyfrowane.
- Przy przesyłaniu danych pracowników, niezbędnych do wykonania przelewów wynagrodzeń, używa się bezpiecznych stron szyfrowanych protokołem SSL oznaczonych jako https:// i podpisanych certyfikatem,
- Do zabezpieczenia sprzętu komputerowego stosowany jest BitLocker, stosuje się także wbudowane systemy operacyjne,
- W ramach ochrony przed atakami hakerskimi stosuje się odpowiednie zabezpieczenia, których szczegółowe dane stanowią informacje niejawne.

Zarządzanie kluczami

Klucze kryptograficzne zmieniane są w momencie identyfikacji incydentu związanego z naruszeniem bezpieczeństwa stosowanych zabezpieczeń kryptograficznych.

Klucze kryptograficzne zmieniane są również w sytuacji gdy zachodzą podejrzenia, że mogły dostać się w posiadanie osób nieupoważnionych i zawsze w sytuacji wygaśnięcia stosunku pracy, gdy zwalniany pracownik miał do nich dostęp.

XIX. Kontrola zgodności

Organizacja zapewnienia zgodność zasad postępowania z przepisami obowiązującego prawa, poprzez identyfikację wymagań prawnych w zakresie bezpieczeństwa informacji.

Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawa karnego lub cywilnego, zobowiązań wynikających z ustaw, zarządzeń lub umów i jakichkolwiek wymagań bezpieczeństwa.

XX. Postanowienia końcowe

Niniejsza Polityka w zakresie bezpieczeństwa informacji jest obowiązująca z dniem zatwierdzenia przez Przedstawiciela Zarządu.

Wszyscy Pracownicy Organizacji są zapoznani z niniejszą Polityką Bezpieczeństwa Informacji, co potwierdzone jest ich własnoręcznym podpisem i tym samym są zobowiązani do przestrzegania jej zasad i realizowania celów w niej zawartych, zgodnie z realizowanym zakresem obowiązków wynikających z zajmowanego stanowiska pracy.

Nieprzestrzeganie niniejszej polityki bezpieczeństwa informacji lub rażące naruszenie jej zasad skutkujące naruszeniem bezpieczeństwa informacji uznanych przez Organizację za ważne lub wrażliwie, będzie skutkowało wyciągnięciem wobec Pracownika, który dopuścił się nadużycia, odpowiednich sankcji karnych, nagan lub kar porządkowych.