POLITYKA BEZPIECZEŃSTWA INFORMACJI

Wydanie: **1**

Spis treści:

1. Wstęp

1.1. Opis Spółki

Pierwsze wzmianki dotyczące wodociągów i sieci w Lubinie pochodzą z przełomu lat 1875/1876 kiedy to, na wniosek Burmistrza Vorwerka, Rada Miejska uchwaliła rozbudowę wodociągu. Miasto przed rozbudową posiadało 4090 mb sieci wodociągowej a w roku 1906 wynosiła 5488 mb. W latach 1883/1884 przystąpiono do budowy sieci kanalizacyjnej. Skanalizowano wówczas ul. Dworcową, następnie Śródmieście i inne części miasta. Długość sieci w roku 1906 wynosiła 13.000 mb. W tym też roku wybudowano i oddano do eksploatacji Zakład Wodociągów na bazie dwóch studni artezyjskich (istniejący do dziś Zakład Uzdatniania Wody nr 1 przy ul. Wierzbowej), oraz wieżę ciśnień. Zakład wodociągowy dostarczał 150 tyś. m3 wody rocznie. Do 1939 roku zarówno sieci wodno-kanalizacyjne, jak i ujęcie wody było rozbudowywane a jego wydajność wzrosła do 1440 m3/dobę. W 1926 roku wybudowano drugi zakład wodociągowy o wydajności 200 m3/dobę również na bazie studni artezyjskich (aktualnie Zakład Uzdatniania Wody nr 2 przy ul. Wójta Henryka został zlikwidowany, a teren wraz z obiektami kubaturowymi przeznaczony do sprzedaży). Obydwa zakłady eksploatowane do 1945 roku.

Po wyzwoleniu Lubina Zakłady Wodociągowe były nieczynne. Uruchomienie zakładu przy l. Wierzbowej nastąpiło w sierpniu 1945 przez Wydział Mechaniczno Budowlany Zarządu Miasta Lubina. Pierwszy dokument pisemny, dotyczący wodociągów dotyczył poszukiwania dokumentacji wodociągów miejskich oraz pozyskania pasów transmisyjnych do napędu pomp. Ostatecznie pasy zostały wykonane z węży strażackich. Z uwagi na brak energii elektrycznej część miasta i ujęcie korzystało z agregatu prądotwórczego, który eksploatowano począwszy od wyzwolenia miasta przez stacjonujące na terenie Lubina jednostki radzieckie a następnie po odkryciu złóż miedzi służył do zaopatrzenia w wodę mieszkańców hoteli robotniczych i obiektów kierownictwa Kombinatu Górniczo-Hutniczego Miedzi. Z chwilą uruchomienie wodociągów rozpoczęto eksploatacje sieci kanalizacyjnych osadników Imhoffa oraz zbiorników bezodpływowych. Pierwszą Oczyszczalnie Ścieków mechaniczno-biologiczną oddano do eksploatacji w 1965 roku o przepustowości 2400 m3/dobę. Oczyszczalnia wybudowana została przydrodze do Ścinawy (część obiektów kubaturowych istnieje do chwili obecnej).

Dynamiczny rozwój miasta Lubina doprowadził do rozbudowy sieci wodociągowych i kanalizacyjnych ujęć i zakładów uzdatniania wody oraz oczyszczalni ścieków. Kolejno powstają:

- Ujęcie i Zakład Uzdatniania Wody nr 3 przy ul. Spacerowej oddany do eksploatacji w 1969 roku;
- Ujęcie i Zakład Uzdatniania Wody nr 4 przy ul. Niepodległości oddany do eksploatacji 31 sierpnia 1976 roku;
- Ujęcie i Zakład Uzdatniania Wody nr 5 przy ul. Gajowej realizowano w latach 1972-1980 (ujęcie Osiek I 1972-74, Ujęcie Osiek II 1974-78, ZUW oddano do eksploatacji w 1980 roku);
- Mechaniczno-Biologiczna Oczyszczalnia Ścieków o przepustowości 27.500 m3/dobę przy ul. Zielonej oddana do eksploatacji w 1974 roku;
- Baza Zaplecza Technicznego i Biurowego Przedsiębiorstwa oddana do eksploatacji w roku 1987 przy ul. Rzeźniczej 1.

W okresie powojennym zarządzanie gospodarką komunalną, w tym Zakładu Wodociągowego przechodziło szereg zmian organizacyjnych. Od maja 1945 roku działalnością wodociągową zajmował się Wydział Mechaniczno-Budowlany przy Zarządzie Miejskim. W sierpniu 1945 roku działalność tę nadzorował Zarząd Nieruchomości podległy Wydziałowi Gospodarki Komunalnej Zarządu Miasta, a od 1949 roku utworzono Zakład Gospodarki Komunalnej. W 1957 roku na bazie Zakładu Gospodarki Komunalnej utworzono Miejskie Przedsiębiorstwo Gospodarki Komunalnej, którego pierwszym dyrektorem został Józef Nojman. W 1973 roku nastąpiła regionalizacja służb komunalnych i z dniem 1 stycznia 1974 roku utworzono Powiatowe Przedsiębiorstwo Komunalne i Mieszkaniowe, obejmujące swym zasięgiem miasta Polkowice, Chocianów i Ścinawę oraz miejscowości wiejskie Rudną i Chobienię. W wyniku kolejnej regionalizacji z dniem 1 stycznia 1975 roku powstało Lubińskie Przedsiębiorstwo Komunalne, które działalność swą prowadziło do dnia likwidacji tj. do 31 marca 1994 roku.

1.2 Definicje

Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji, czyli informacja nie jest ujawniana osobom nieupoważnionym, jest ona dokładna i kompletna oraz dostępna i użyteczna na żądanie upoważnionego personelu.

Ryzyko – prawdopodobieństwo wystąpienia zagrożenia, które, wykorzystując podatność(ci) aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia.

Szacowanie ryzyka – całościowy proces analizy i oceny ryzyka.

Aktyw/zasób – wszystko to, co ma wartość dla organizacji.

Poufność – zapewnienie dostępu do informacji tylko osobom upoważnionym.

Integralność – zapewnienie dostępu do informacji tylko osobom upoważnionym.

Dostępność – zapewnienie, że osoby upoważnione będą miały dostęp do informacji tylko wtedy gdy jest to uzasadnione.

Postępowanie z ryzykiem – proces wyboru i wdrażania środków modyfikujących ryzyko.

Zarządzanie ryzykiem – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów.

Zdarzenie związane z bezpieczeństwem informacji – zdarzenie związane z bezpieczeństwem informacji jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

Incydent związany z bezpieczeństwem informacji – incydent związany z bezpieczeństwem informacji jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

Ryzyko szczątkowe – ryzyko pozostające po procesie postępowania z ryzykiem.

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

2. Zakres Systemu Bezpieczeństwa Informacji

System Zarządzania Bezpieczeństwa Informacji (SZBI) w Spółce stanowi część całościowego systemu zarządzania, opartą na podejściu wynikającym z ryzyka biznesowego, odnoszącą się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. System Zarządzania Bezpieczeństwem Informacji (SZBI) został opracowany, wdrożony i jest utrzymywany w MPWiK Sp. z o. o. w Lubinie w oparciu o normę PN-ISO/IEC 27001:2007. Zakres SZBI dotyczy procesów prowadzonej działalności w dziedzinie produkcji, uzdatniania i dostarczania wody, odbioru i oczyszczania ścieków, projektowania i wykonawstwa przyłączy wodno-kanalizacyjnych oraz laboratoryjnych analiz wody i ścieków.

3. Deklaracja Zarządu

Najwyższe kierownictwo Spółki, stojąc na stanowisku, że informacja jest priorytetowym zasobem każdej organizacji, wdrożyło w ramach ZSZ system zarządzania bezpieczeństwem informacji. Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów naszej Spółki oraz warunkiem ciągłego jej rozwoju. Gwarancją sprawnej i skutecznej ochrony informacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa oraz zastosowanie rozwiązań technicznych.
Zarząd Spółki wprowadzając Politykę Bezpieczeństwa Informacji, deklaruje, że wdrożony System Zarządzania Bezpieczeństwem Informacji będzie podlegał ciągłemu doskonaleniu zgodnie z wymaganiami normy PN-ISO/IEC 27001:2007.

Podejście do bezpieczeństwa informacji w Spółce opiera się na trzech kluczowych regułach:

- **Reguła poufności informacji** - zapewnienie, że informacja jest udostępniana jedynie osobom upoważnionym
- **Reguła integralności informacji** - zapewnienie zupełnej dokładności i kompletności informacji oraz metod jej przetwarzania
- **Reguła dostępności informacji** - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba

Celem wdrożonego systemu zarządzania bezpieczeństwem informacji jest osiągnięcie poziomu organizacyjnego i technicznego, który:

- będzie gwarantem pełnej ochrony danych Klientów oraz ciągłość procesu ich przetwarzania,
- zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych oraz jawnych,
- zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania,
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualne wykorzystanie na szkodę Spółki,
- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa Spółki, jej interesów oraz posiadanych i powierzonych jej informacji.

Powyższe cele realizowane są poprzez:

- wyznaczenie osób odpowiedzialnych zapewniających optymalny podział i koordynację zadań związanych z zapewnieniem bezpieczeństwa informacji,
- wyznaczenie właścicieli dla kluczowych aktywów przetwarzających informację, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu bezpieczeństwa,
- przyjęcie za obowiązujące przez wszystkich pracowników polityk i procedur bezpieczeństwa obowiązujących w Spółce,
- określeniu zasad przetwarzania informacji, w tym stref w których może się ono odbywać,
- przegląd i aktualizację polityk i procedur postępowania dokonywaną przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty,
- ciągłe doskonalenie systemu zapewnia bezpieczeństwa informacji funkcjonującego w Spółce zgodnie z wymaganiami normy PN-ISO/IEC 27001:2007 i zaleceniami wszystkich zainteresowanych stron.

Prezes Zarządu

Jarosław Wantuła

4. Zasady ogólne

Każdy pracownik Spółki jest zapoznawany z regułami oraz z aktualnymi procedurami ochrony informacji w swojej komórce organizacyjnej. Poniższe uniwersalne zasady są podstawą realizacji polityki bezpieczeństwa informacji:

- **Zasada uprawnionego dostępu.** Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności.
- **Zasada przywilejów koniecznych**. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
- **Zasada wiedzy koniecznej**. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
- **Zasada usług koniecznych**. Spółka świadczy tylko takie usługi jakich wymaga Klient.
- **Zasada asekuracji**. Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym. W przypadkach szczególnych może być stosowane dodatkowe niezależne zabezpieczenie.
- **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych Spółki i aktywnie uczestniczą w tym procesie.
- **Zasada indywidualnej odpowiedzialności**. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
- **Zasada obecności koniecznej**. Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
- **Zasada stałej gotowości**. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
- **Zasada kompletności**. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
- **Zasada odpowiedniości**. Używane mechanizmy muszą być adekwatne do sytuacji.
- **Zasad akceptowanej równowagi**. Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji.

5. Organizacja bezpieczeństwa informacji

5.1. Struktura zarządzania bezpieczeństwem

Wszystkie procesy bezpieczeństwa, rozwiązania techniczne oraz jego organizacja muszą być zgodne z następującymi zasadami:

- bezwzględne oddzielenie funkcji zarządzających i kontrolnych od funkcji wykonawczych,
- uniemożliwienie nadużyć i maksymalne ograniczenie błędów popełnianych przez pojedyncze osoby w sferze jednoosobowej odpowiedzialności,
- zapewnienie niezależności i bezinteresowności jednostek dokonujących audytu bezpieczeństwa przy zapewnieniu rękojmi zachowania tajemnicy.

5.2. Dokumentacja systemu zarządzania bezpieczeństwem informacji

Dokumentacja systemu zarządzania bezpieczeństwem składa się z czterech głównych elementów. Są nimi:

- Polityka Bezpieczeństwa Informacji
- Księga Bezpieczeństwa Informacji
- Deklaracja Stosowania Zabezpieczeń
- Procedury i instrukcje bezpieczeństwa, które określają szczegółowo zasady postępowania
- Raporty z analizy ryzyka i plany postępowania z ryzykiem

Uzupełnieniem dokumentacji SZBI jest dokumentacja z funkcjonującego Systemu Zarządzania Jakością.

5.3. Struktura zarządzania bezpieczeństwem informacji

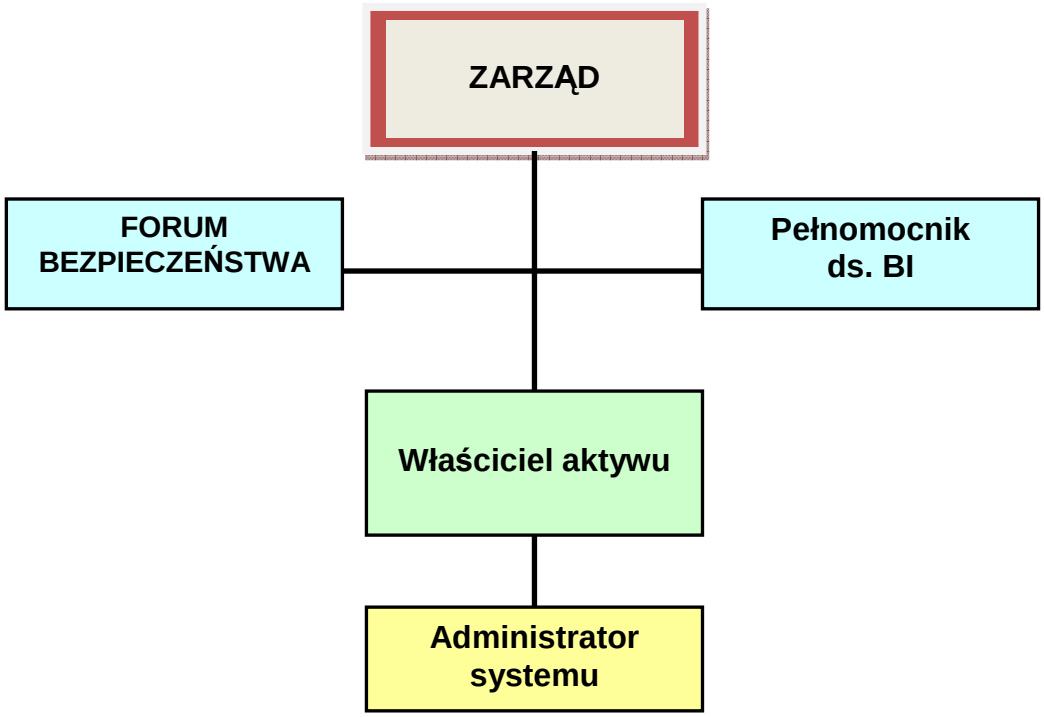
Odpowiedzialność za bezpieczeństwo informacji w Spółce ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków.

- Kierownictwo firmy odpowiedzialne jest za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz poszczególnych zabezpieczeń. Wydaje zgodę na użyt-

kowanie urządzeń służących do przetwarzania informacji i zabezpieczeń rekomendowanych przez Forum Bezpieczeństwa. Decyduje również o współpracy w zakresie bezpieczeństwa z innymi podmiotami. Kierownictwo może również wyrazić zgodę na udostępnienie stronom trzecim informacji stanowiących tajemnicę firmy.

- Pełnomocnik ds. Bezpieczeństwa Informacji odpowiedzialny jest za wdrożenie i koordynację zapewnienia bezpieczeństwa informacji oraz związanych z nim polityk i procedur.
- Forum Bezpieczeństwa jest organem doradczym w Spółce w zakresie zagadnień związanych z bezpieczeństwem informacji.
- Właściciel aktywu odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem.
- Administrator aktywu odpowiada za realizację i nadzór nad technicznymi aspektami aktywu w ścisłej kooperacji z Właścicielem aktywu.

Poniższy schemat przedstawia organizację zarządzania bezpieczeństwem informacji w Spółce.



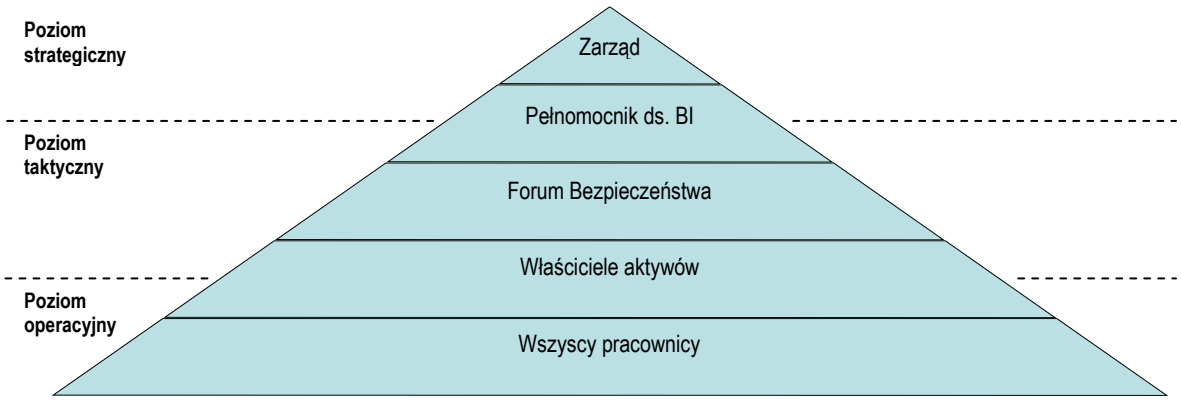
W powyższej strukturze możliwe jest wyróżnienie trzech poziomów działań:

- Na **poziomie strategicznym** prowadzona jest generalna polityka bezpieczeństwa informacji w odniesieniu do wcześniej rozpoznanego, określonego, a także poddanego analizie ryzyka i zasadniczych oczekiwań, co do poziomu bezpieczeństwa informacji oraz w odniesieniu do wynikających z nich modelowych zadań i rozwiązań. Dlatego też w procesy decyzyjne tego poziomu zaangażowane jest najwyższe kierownictwo Spółki określające zasadnicze użytkowe kryteria bezpieczeństwa informacji (pochodne od kryte-

riów normatywnych i możliwe do zrealizowania na bazie zidentyfikowanych atrybutów informacji) .

- Na **poziomie taktycznym** tworzone są standardy bezpieczeństwa informacji oraz zasady kontroli ich wypełniania w stosowanych rozwiązaniach i systemach informatycznych oraz przestrzegania w praktyce używania tych rozwiązań i systemów (stosownie do założonych poziomów bezpieczeństwa: standardowego, podwyższonego lub specjalnego). W te procesy decyzyjne zaangażowane jest (głównie) kierownictwo.
- Na **poziomie operacyjnym** prowadzona jest administracja bezpieczeństwem informacji pod kątem pełnego stosowania standardów bezpieczeństwa oraz rozwiązywania sytuacji zakłóceń wynikających z naruszenia tych standardów (intencjonalnego lub przypadkowego).

Diagram przedstawiony poniżej prezentuje graficznie przedstawiony podział.



5.4. Funkcjonowanie forum bezpieczeństwa

5.4.1. Organizacja Forum Bezpieczeństwa

W skład Forum wchodzi Prezes Zarządu, Pełnomocnik ds. Bezpieczeństwa Informacji oraz inni pracownicy powołani przez Prezesa Zarządu. Forum zwoływane jest przez Pełnomocnika ds. Bezpieczeństwa Informacji za zgodą Prezesa Zarządu.

5.4.2. Zadania, uprawnienia i odpowiedzialność Forum Bezpieczeństwa

- dokonywanie przeglądu polityki bezpieczeństwa informacji oraz ogólnego podziału odpowiedzialności,
- uzgadnianie metodyki i procesów związanych z bezpieczeństwem informacji (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,

5.5. Zasady współpracy z osobami trzecimi

Każdy gość lub osoba, która wykonuje prace zlecone na terenie firmy zobligowana jest do przestrzegania następujących procedur:

- do podpisania umowy lojalnościowej o przestrzeganiu tajemnicy służbowej,
- do podpisania odpowiedzialności za naruszenie obowiązków pracowniczych/ zleceniobiorcy i za szkodę wyrządzoną pracodawcy/ zleceniodawcy,
- do przestrzegania reguł bhp,
- do przestrzegania reguł bezpieczeństwa przeciwpożarowego.

Każda osoba trzecia, która narusza sferę bezpieczeństwa Spółki nie zostaje pozostawiona bez nadzoru personelu firmy. Dostęp do magazynów i biur wszelkiego personelu technicznego zajmującego się konserwacją sprzętu, ochrony i innych osób jest nadzorowany przez pracowników Spółki. Spółka kieruje się zasadą, że najbardziej zaufanymi osobami trzecimi

są już znane osoby firmie, które wcześniej były już obecne na terenie firmy. Dostęp gości w strefie bezpieczeństwa jest możliwy tylko i wyłącznie w godzinach pracy.

5.6. Zasady współpracy ze stronami zewnętrznymi

Współpraca firmy z innymi spółkami oparta jest na umowach. Zawierając te umowy Spółka ma zawsze na względzie, aby obejmowały one deklarację o zachowanie poufności oraz zobowiązania do działania zgodnie z prawem.

5.7. Zasady współpracy z Policją, jednostkami Straży Pożarnej i Straży Miejskiej

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 na obiekcie.
- 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 jednostki na wypadek pożaru lub awarii:

- zaistniałym pożarze lub awarii pracownik natychmiast zawiadamia Straż Pożarną oraz osobę odpowiedzialną za obiekt,
- przybyłe jednostki ratownicze natychmiast kieruje na miejsce akcji.

6. Zarządzanie aktywami i ryzykami

Spółka zarządza swoimi aktywami informacyjnymi poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. Identyfikowane są aktywa informacyjne i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony.

Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji w całej firmie jest przeprowadzanie okresowej analizy ryzyka i opracowania planów postępowania z ryzykiem. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów Spółki.

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 kierownictwa oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

6.1. 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. O ile nie zostało to określone szczegółowo w innych opracowaniach, za dopuszczenie do użytkowania nowych urządzeń odpowiada Pełnomocnik ds. Bezpieczeństwa Informacji.

7. Bezpieczeństwo zasobów ludzkich

Spółka dba o zapewnienie kompetentnych pracowników do realizacji wyznaczonych w procesach zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Zasoby ludzkie są również ważnym czynnikiem analizowanym podczas przeprowadzania okresowej analizy ryzyka. Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonym procedurom rozwiązywania umów o pracę.

8. Bezpieczeństwo fizyczne i środowiskowe

Spółka dba o zapewnienie wysokiego poziomu bezpieczeństwa fizycznego i środowiskowego. Celem takiego postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami w obiektach Spółki. W przypadku informacji i danych od naszych Klientów najistotniejsze jest zapewnienie wszystkich trzech podstawowych aspektów bezpieczeństwa poufności danych oraz ich dostępności i integralności. 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. Kluczowe systemy techniczne i informatyczne wyposażone są w systemy podtrzymujące zasilanie.

9. Zarządzanie systemami i sieciami

Spółka dba o przestrzeganie zasad związanych z utrzymywaniem i użytkowaniem systemów informatycznych i sieci. Celem takiego postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez nie informacji własnych.
Skuteczna realizacja postawionego celu możliwa jest dzięki:

- kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami administrującymi zasobami informatycznymi i wspomagającymi Spółki,
- opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy,
- kontrolowaniu wprowadzania wszelkie zmian do infrastruktury technicznej,
- w celu zapewnienia bezpieczeństwa systemów produkcyjnych, prace rozwojowe i testowe prowadzone są na oddzielnych urządzeniach lub środowiskach,
- usługi dostarczane przez strony trzecie są nadzorowane, w szczególności wszelkie wprowadzane do nich zmiany. Po zakupie, lub wprowadzeniu zmiany do systemu jest on odbierany i akceptowany w sposób świadomy, uwzględniający jego wpływ na istniejący system bezpieczeństwa,
- wdrożone są zabezpieczenia chroniące przed oprogramowaniem złośliwym i mobilnym,
- 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,

Spółka monitoruje poziom incydentów w systemach informatycznych i posiada mechanizmy reagowania w przypadkach ich wystąpienia.

10. Wymiana informacji

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

11. Kontrola dostępu

Spółka zarządza kontrolą dostępu. Celem takiego postępowania jest zapewnienie, że dostęp do informacji, miejsc, urządzeń lub systemów ich przetwarzania mają tylko osoby uprawnione. Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z nadzorowaniem ruchu osobowego.

12. Utrzymanie systemów informacyjnych

Spółka zapewnia, że wszystkie procesy związane z pozyskaniem, rozwojem bądź utrzymaniem systemów informacyjnych prowadzone są w sposób nadzorowany, gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa. Na to zapewnienie składa się:

- uwzględnianie wymogów bezpieczeństwa podczas zakupu lub produkcji nowych systemów,
- dopuszczenie nowego systemu poprzedzone jest zawsze fazą testowania,
- nadzorowanie dostępu do kodów źródłowych oprogramowania,
- wdrożone procedury kontroli zmian/ aktualizacji oprogramowania.

13. Zarządzanie incydentami

W przypadku wszelkich incydentów w Spółce powiadamiany jest Pełnomocnik ds. Bezpieczeństwa Informacji. 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 usunąć ewentualne skutki zaistnienia incydentu, a następnie wszystkie incydenty są szczegółowo analizowane i podejmowane są dalsze decyzje właściwe dla danej sytuacji. Incydenty są rejestrowane i analizowane przez Pełnomocnika ds. Bezpieczeństwa Informacji i członków Forum Bezpieczeństwa.

14. Zarządzanie ciągłością działania

Spółka dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności biznesowej oraz ochrona krytycznych procesów biznesowych przed rozległymi awariami lub katastrofami. Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z zarządzeniem ciągłością działania tak, aby ograniczać do akceptowalnego poziomu skutków wypadków i awarii. W sposób systemowy tworzone są plany postępowania w sytuacjach kryzysowych. Powołane Forum Bezpieczeństwa dba o ich aktualność i testuje je pod względem przydatności w sytuacji realnego zagrożenia. Powyższe zasady zapewniają, że firma jest przygotowana na działanie również w przypadkach odbiegających od normy.

15. Zgodność z wymaganiami prawnymi i innymi

Spółka dba o zapewnienie zgodności zasad postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych własnych standardów. Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawa karnego lub cywilnego, zobowiązań wynikających z ustaw, zarządzeń lub umów i jakichkolwiek wymagań bezpieczeństwa. Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z identyfikacja wymagań prawnych w zakresie bezpieczeństwa informacji. Prowadzony jest nadzór nad komplementarnością stosowanych techniczną urządzeń oraz prowadzone są audyty wewnętrzne funkcjonowania systemu.

16. Postanowienia końcowe

Spółka wymaga zapoznania się pracowników z dokumentacją Polityki Bezpieczeństwa Informacji. Za złożenie przez nich stosownych oświadczeń oraz uzyskanie niezbędnych praw dostępu (do pomieszczeń i systemów informatycznych), stosownie do przypisanej roli odpowiada bezpośredni przełożony.

Bieżący nadzór nad przestrzeganiem przyjętych zasad w zakresie bezpieczeństwa informacji pełni Pełnomocnik ds. Bezpieczeństwa Informacji, będący reprezentantem Zarządu Spółki.

Naruszenia świadome, bądź przypadkowe niniejszej Polityki Bezpieczeństwa Informacji (wraz z wszystkimi dokumentami operacyjnymi) powoduje skutki prawne zgodnie z Regulaminem Pracy, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez sąd.

17. Historia zmian

Nr zmiany	Data zmiany	Opis zmiany	Obowiązujące wydanie