Opracował: Katarzyna Cichewicz	01.07.2024	Podpis:
Zatwierdził: Marcin Orchel	01.07.2024	Podpis:

1. Wstęp

1.1. Bezpieczeństwo i niezawodność

Zapewniamy naszym Klientom najwyższy stopień bezpieczeństwa i niezawodności.

1.2. Definicja bezpieczeństwa i zakres systemu

Celem Systemu Zarządzania jest zapewnienie bezpieczeństwa informacjom chronionym, zarówno własnym jak i powierzonym przez klientów, w tym danych osobowych, poprzez zapewnienie tym informacjom cech: poufności, integralności oraz dostępności.

Zakresem systemu objęte są informacje przetwarzane w ramach działań:

Świadczenie usług medycznych w zakresie rehabilitacji leczniczej

30-053 Kraków, ul. Kronikarza Galla 24/203

32-100 Łaganów, Łaganów 22

1.3. Deklaracja Najwyższego Kierownictwa

Bezpieczeństwo informacji, systemów oraz chmur, w których są one przetwarzane jest jednym z kluczowych elementów jakości oferowanej Klientom oraz warunkiem ciągłego rozwoju Organizacji. Gwarancją sprawnej i skutecznej ochrony informacji jest zapewnienie odpowiedniego poziomu kultury bezpieczeństwa oraz zastosowanie przemyślanych rozwiązań technicznych.

Najwyższe Kierownictwo Organizacji wprowadzając Politykę Bezpieczeństwa Informacji, deklaruje, że wdrożony System Zarządzania Bezpieczeństwem Informacji będzie podlegał ciągłemu doskonaleniu zgodnie z wymaganiami normy ISO/IEC 27001. Zakres zarządzania bezpieczeństwem informacji obejmuje dane i informacje powierzone przez naszych Klientów oraz informacje własne Organizacji przetwarzane we wszystkich procesach.

Podejście do bezpieczeństwa informacji w Organizacji wywodzi się z trzech kluczowych kwestii:

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

Celem wdrożonego Systemu Zarządzania Bezpieczeństwem informacji jest osiągnięcie takiego 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 Organizacji,
- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa Organizacji, jej interesów oraz posiadanych i powierzonych jej informacji.

Powyższe cele realizowane są poprzez:

- wyznaczenie struktury organizacyjnej zapewniającej optymalny podział i koordynację zadań i odpowiedzialności 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 Organizacji,
- podziale informacji na klasy i przyporządkowanie im zasad postępowania,
- 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 Organizacji zgodnie z wymaganiami normy SO/IEC 27001, zaleceniami wszystkich zainteresowanych stron oraz innymi wymaganiami.

2. Organizacja bezpieczeństwa informacji

Przyjmuje się, że podstawowymi zasadami przy tworzeniu struktur zarządzających bezpieczeństwem są:

- 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 auditu bezpieczeństwa przy zapewnieniu rękojmi zachowania tajemnicy.

Wszystkie procesy bezpieczeństwa, a także rozwiązania bezpieczeństwa oraz organizacja jego zapewniania, muszą być zgodne z powyższymi zasadami.

2.1. Struktura zarządzania bezpieczeństwem i podział odpowiedzialności

1. Odpowiedzialność za bezpieczeństwo informacji w organizacji ponosi cały personel.
2. Kierownictwo firmy odpowiedzialne jest za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia SZBI oraz poszczególnych zabezpieczeń. Wydaje zgodę na użytkowanie urządzeń przetwarzania informacji i zabezpieczeń. Decyduje również o współpracy w zakresie bezpieczeństwa z innymi podmiotami. Kierownictwo może również wyrazić zgodę na udostępnienie stronom trzecim informacji stanowiących tajemnicę firmy. Jego codzienne postępowanie stanowi przykład dla całego personelu, że aspekty bezpieczeństwa informacji posiadają wysoki priorytet we wszystkich podejmowanych i planowanych działaniach.
3. Pełnomocnik odpowiedzialny jest za wdrożenie i realizację działań zapewniających bezpieczeństwo informacji oraz przestrzeganie związanych z nim polityk i procedur.
4. Administrator Systemów odpowiada za wdrożenie i realizację oraz wypracowywanie i nadzór nad realizacją procedur w zakresie bezpieczeństwa systemów informatycznych.
5. Właściciel zasobu oraz Administrator Systemów jest odpowiedzialny za zapewnienie przestrzegania przez podległy sobie dział, zespół polityki bezpieczeństwa informacji oraz procedur szczegółowych w tym dotyczących zasad postępowania z informacją chronioną oraz zasad rejestracji i postępowania z naruszeniami.

2.2. Podział obowiązków

Najwyższe Kierownictwo (Kierownik podmiotu, prokurent, koordynator podmiotu leczniczego) odpowiada za:

- Całość bezpieczeństwa informacji;
- Za nadzór nad realizacją polityki bezpieczeństwa informacji oraz innych dokumentów wewnętrznych związanych z ochroną informacji;
- Decydowanie o współpracy w zakresie bezpieczeństwa z innymi podmiotami;
- Wyrażanie zgody na udostępnienie stronom trzecim informacji stanowiących tajemnicę organizacji;
- Za wyznaczenie pełnomocnika oraz właścicieli aktywów;
- Uczestniczy w opracowaniu szczególnych wymagań bezpieczeństwa i procedur bezpieczeństwa;
- Zapewnienie przetwarzania danych osobowych zgodnie z ustawą o ochronie danych osobowych oraz innymi przepisami powszechnie obowiązującego prawa;

Najwyższe Kierownictwo, Pełnomocnik oraz Właściciele Aktywów koordynują działania w zakresie bezpieczeństwa poprzez:

- Wskazywanie kierunków działań w zakresie bezpieczeństwa;
- Wykonywanie przeglądów polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji;
- Monitorowanie istotnych zmian narażenia aktywów informacyjnych na zagrożenia;
- Wykonywanie przeglądu i monitorowanie naruszeń bezpieczeństwa informacji;
- Dokonywanie analizy naruszeń bezpieczeństwa informacji.
- Spotkania na przeglądach zarządzania oraz doraźne w sytuacjach mogących mieć istotny wpływ na bezpieczeństwo informacji;

- Monitorowanie zmian w przepisach prawnych dotyczących sposobu zabezpieczenia danych oraz dostosowanie systemu do wymagań prawnych;
- Monitorowanie, zarządzanie, weryfikację i nadzór nad bezpieczeństwem informacji przetwarzanych w chmurach

Pełnomocnik jest odpowiedzialny za:

- Nadzór nad przestrzeganiem zasad ochrony informacji obowiązujących w Organizacji;
- Koordynację zapewnienia bezpieczeństwa informacji oraz związanych z nim polityk i procedur;
- Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń bezpieczeństwa informacji lub prób takich naruszeń;
- Rozstrzyganie problemów dotyczących wątpliwości w stosowaniu dokumentacji systemu;
- Przestrzeganie zasad ochrony informacji przez niego jak i przez personel
- Identyfikowanie i dokumentowanie zagrożeń zachowania bezpieczeństwa informacji,
- Definiowanie oraz realizację działań zapobiegających zagrożeniom,
- Zapoznanie personelu z obowiązkami związanymi z ochroną informacji na stanowiskach pracy;
- Kontroluje znajomość procedur bezpieczeństwa przez wszystkich użytkowników systemu w zakresie bezpieczeństwa teleinformatycznego;
- Prowadzi nadzór nad kontrolą uprawnień w zakresie zarządzania chmurą

Administrator Systemu – odpowiada za:

- Nadawanie i odbieranie uprawnień, do korzystania z danych w systemach oraz w chmurach. W tym nadzór nad użytkownikami posiadającymi uprawnienia administratorskie do systemów oraz w chmurach.
- Prowadzi bieżącą kontrolę zabezpieczeń oraz zgodność funkcjonowania systemu ze szczególnymi wymaganiami bezpieczeństwa;
- Wdraża procedury ochrony antywirusowej, przed złośliwym oprogramowaniem oraz nieuprawnionym dostępem do zasobów systemów oraz w chmurach za pośrednictwem sieci teleinformatycznych;
- Sprawdza poprawność działania systemu oraz jego zabezpieczeń w zakresie ochrony antywirusowej, przed złośliwym oprogramowaniem oraz innymi zagrożeniami mogącymi pochodzić z sieci teleinformatycznych;
- Uczestniczy w opracowaniu szczególnych wymagań bezpieczeństwa i procedur bezpieczeństwa;
- Analizę pracy systemu informatycznego w celu wykrycia potencjalnych zagrożeń;

Właściciele aktywów – odpowiadają za:

- Bezpieczeństwo informacji w zakresie nad którym sprawują nadzór;
- Przeciwdziałanie dostępowi do informacji chronionych osób niepowołanych;
- Decydowanie o współpracy w zakresie bezpieczeństwa z innymi podmiotami, w zakresie nad którym sprawują nadzór;
- Wyrażanie zgody na udostępnienie stronom trzecim informacji chronionych należących do aktywa, którego są właścicielami;
- Podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie oraz zasobach chmurowych;

- Zapewnienie przetwarzania danych osobowych zgodnie z ustawą o ochronie danych osobowych;
- Bieżące nadzorowanie oraz zarządzanie aktywem jako właściciele aktywów;
- Nadzór nad poprawnością pracy systemów informatycznych oraz mechanizmów zabezpieczających dane w tych systemach;
- Nadzór nad zabezpieczeniem danych poprzez tworzenie i właściwe zabezpieczanie kopii zapasowych;
- Analizę pracy systemu informatycznego w celu wykrycia potencjalnych zagrożeń;
- Nadzór nad przeprowadzaniem w bezpieczny sposób napraw oraz konserwacji sprzętu i oprogramowania służącego do przetwarzania lub będącego nośnikiem danych;
- Utrzymywanie ochrony aktywów i zasobów, którymi dysponują;
- Wprowadzanie zabezpieczeń;
- Utrzymanie aktualnych wersji oprogramowania oraz dokumentacji eksploatacyjnej;
- Wnioskowanie o nadanie lub odebranie uprawnień
- Prowadzenie dokumentacji systemu;
- Przegląd i weryfikację efektywności ustanowionego systemu i informowanie podczas przeglądu o jej wynikach;
- Propagowanie zasad systemu zarządzania bezpieczeństwem informacji wśród personelu w podległych im obszarach;
- Nadzorowanie realizacji założeń polityki bezpieczeństwa informacji i innych dokumentów systemu bezpieczeństwa informacji w podległych obszarach.

Personel

- Odpowiedzialność za bezpieczeństwo informacji ponosi cały personel zgodnie z posiadanym zakresem obowiązków. Każdy personel zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi przepisami wewnętrznymi w tym m. in.
- Stosować zasady opisane w Polityce oraz innych dokumentach wewnętrznych;
- Chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych;
- Chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją;
- Chronić sprzęt, nośniki magnetyczne i wydruki komputerowe zawierające dane chronione;
- Utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu;
- Stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do innych zaleceń wynikających z Systemu Zarządzania Bezpieczeństwem Informacji;
- Powiadomić Pełnomocnika, bezpośredniego przełożonego:
    - Ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym;
    - Nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian;
    - Zniszczeniu lub możliwości zniszczenia informacji chronionych;
    - Zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych;

Zabrania się pod rygorem odpowiedzialności służbowej i karnej:

- Ujawniać informacje chronione (w tym dane osobowe),

- Kopiować bazy danych lub ich części poza kopiami przewidzianymi dokumentacją systemu zarządzania bezpieczeństwem informacji jak np. Kopie bezpieczeństwa,
- Uszkadzać lub niszczyć sprzęt lub informacje bez zachowanych odpowiednich procedur bezpieczeństwa,
- Zabrania się przetwarzania informacji chronionych w sposób mogący narażać na utratę bezpieczeństwa tych danych przez naruszenie poufności, integralności lub dostępności,
- Instalowania oprogramowania niezwiązanego z wykonywaniem obowiązków służbowych

2.3. Analiza Ryzyka

Podstawowym elementem budowy systemu jest analiza ryzyka. Organizacja szacujący ryzyko wzięła pod uwagę wymagania z załącznika A normy ISO 27001. Plany postępowania z ryzykiem zostały opracowane w korelacji ze słabościami wynikającymi z deklaracji stosowania.

2.4. Kontrola dostępu

Organizacja 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 w wyznaczonych strefach bezpieczeństwa.

Największa uwaga poświęcona jest kontroli dostępu do danych powierzonych przez Klientów.

Organizacja prowadzi okresową kontrolę praw dostępu w tym celu Właściciel aktywu (systemu) nie rzadziej niż raz na rok przeprowadza kontrolę aktualności i poprawności listy zarejestrowanych w systemie użytkowników i przypisanych im praw dostępu.

2.4.1. Kontrola dostępu do pomieszczeń biurowych.

Dostęp do biura jest zabezpieczony alarmem, monitoringiem oraz kontrolą dostępu. Przychodnia jest zamykana drzwiami z zamkiem.

Drzwi oddzielające przestrzeń ogólnodostępną od gabinetów również są zabezpieczone kontrolą dostępu, każde pomieszczenie ma zamek i może być zamykane na klucz.

2.4.2. Zasady nadawania uprawnień użytkowników

Udzielanie, zmiana i odbiór uprawnień użytkowników jest wykonywane przez Administratora Systemu na wniosek Pełnomocnika lub Kierownika Placówki.

W przypadku rejestrowania konta nowego użytkownika w systemie, identyfikator i hasło początkowe musi mu być przekazane w sposób uniemożliwiający użycie tych informacji przez osoby nieuprawnione. Nowy użytkownik jest zobowiązany do zmiany hasła już przy pierwszym zalogowaniu do systemu.

2.4.3. Zasady i korzystanie z haseł w systemach informatycznych

Dostęp do systemu informatycznego przetwarzającego chronione dane możliwy jest wyłącznie dla zarejestrowanych użytkowników po podaniu identyfikatora oraz hasła. Identyfikator jest unikalny dla każdego użytkownika systemu.

Hasło jest znane tylko przez użytkownika.

Polityka nadawania haseł opisana jest w procedurach PBI - 06 Korzystanie z zasobów informatycznych przez użytkowników oraz PBI - 07 Korzystanie z zasobów - administratorzy.

Użytkownik hasła zobowiązany jest do:

- nieujawniania hasła innym osobom,
- zachowania hasła w tajemnicy również po wygaśnięciu jego ważności,
- niezapisywania hasła w miejscach dostępnych dla osób nieuprawnionych,

2.5. Bezpieczeństwo fizyczne i środowiskowe

Organizacja dba o zapewnienie wysokiego poziomu bezpieczeństwa fizycznego i środowiskowego. Celem takiego postępowania jest ochrona informacji przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami w siedzibie Organizacji. W przypadku danych od naszych Klientów najistotniejsze jest zapewnienie wszystkich trzech podstawowych aspektów bezpieczeństwa: poufności, dostępności i integralności. Podobnie sytuacja wygląda w przypadku danych własnych.

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. Wyznaczone są obszary dostawy pozwalające na bezpieczny wyładunek materiałów przywiezionych od dostawcy.

Każdy z pracowników przypisane ma swoje osobiste konto pracy.

Organizacja kieruje się następującą zasadą: **„Blokuj dostęp do wszystkich miejsc przetwarzania informacji poza wyraźnie dozwolonymi, bo od tego zależy bezpieczeństwo również Twoich chronionych informacji**”.

2.6. Zarządzanie aktywami i ryzykami

Ewidencja aktywów informatycznych przetwarzających informacje (urządzenia, oprogramowanie, informacje) prowadzona jest przez Pełnomocnika. Lista aktywów zawiera dane identyfikacyjne aktywów, oraz określa właściciela aktywu. Aktualizacja Listy aktywów przetwarzających informacje odbywa się na podstawie wniosków kierowników odpowiedzialnych za obszary funkcjonalne – właścicieli aktywów.

Organizacja uważnie zarządza swoimi aktywami informacyjnymi. Celem takiego postępowania jest zapewnienie im wymaganego poziomu bezpieczeństwa.

Identyfikowane są aktywa informacyjne i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony. Szczególnie traktowane są kluczowe informacje. Określone są szczegółowe zasady postępowania z danymi grupami informacji oraz grupy pracowników posiadające do nich dostęp.

Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji w całej organizacji jest przeprowadzanie okresowej analizy ryzyka i opracowania planów 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 kierownictwa oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

2.6.1. Zarządzanie nośnikami wymiennymi

W Organizacji obowiązuje zakaz korzystania z wymiennych nośników informacji. Każdorazowe skorzystanie z nośnika wymaga zgody Kierownika Placówki .
W przypadku takiej zgody: Wymienne nośniki informacji muszą być opisane w sposób umożliwiający identyfikację zawartości nośnika, jeśli posiadają informacje chronione, nie mogą one być wynoszone poza siedzibę Organizacji. Działania z nośnikami opisane są w procedurach: PBI - 06 Korzystanie z zasobów informatycznych przez użytkowników oraz PBI - 07 Korzystanie z zasobów - administratorzy

2.7. Przekazywanie informacji - komunikacja

Organizacja komunikuje na zewnątrz tylko informacje, których komunikację umożliwiają przepisy prawa. Zasady SZBI oraz informacje powierzone przez klientów nie są komunikowane na zewnątrz.

Wewnątrz organizacji komunikowane są pojawiające się problemy, incydenty bezpieczeństwa oraz funkcjonujące procedury. Za komunikowanie tych elementów odpowiada Pełnomocnik . Komunikacja odbywa się mailowo lub podczas spotkań z pracownikami.

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.

2.7.1. Zasady współpracy z władzami

Organizacja w ramach prowadzonej działalności utrzymuje kontakt z:
- Policją oraz organami ścigania
- Jednostkami Straży Pożarnej
- Straży Miejskiej
- UODO.

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.

Współdziałanie w celu utrzymania spokoju i porządku publicznego w czasie organizowanych imprez masowych w rejonie obiektu odbywa się poprzez:
- Uzgodnienie zasad współpracy przed planowaną imprezą.
- Informowanie o wszelkich próbach zakłócenia porządku służb patrolowych i dyżurnych Policji.
- Niezwłocznego przekazania Policji osób stwarzających w sposób oczywisty zagrożenie dla życia lub zdrowia ludzkiego, a także chronionego obiektu.

Współdziałanie w celu zmniejszenia skutków incydentu bezpieczeństwa informacji odbywa się poprzez:
- zgłoszenie incydentu do UODO
- przeprowadzenie postępowania wyjaśniającego wystąpienie incydentu bezpieczeństwa informacji
- przeprowadzenie działań następczych

Zabezpieczenie mienia jednostki na wypadek pożaru lub awarii:
- Zaistniałym pożarze lub awarii pracownik natychmiast zawiadamia Straż Pożarną oraz Najwyższe kierownictwo.
- Przybyłe jednostki ratownicze natychmiast kieruje na miejsce akcji.

2.7.2. Zasady współpracy z osobami trzecimi

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

- do podpisania deklaracji o poufności, jeżeli wiąże się to z dostępem do informacji,
- do przestrzegania reguł bhp,
- do przestrzegania reguł bezpieczeństwa przeciwpożarowego,
- zakazu wynoszenia danych

Każda osoba trzecia, która narusza sferę bezpieczeństwa nie zostaje pozostawiona bez nadzoru personelu Organizacji. Dostęp do magazynów i biur wszelkiego personelu technicznego zajmującego

się konserwacją sprzętu, ochrony, partnerów handlowych i innych osób jest nadzorowany przez pracowników Organizacji.

2.7.3. Zasady współpracy z innymi Organizacjami

Współpraca Organizacji z innymi Organizacjami oparta jest na umowach. Zawierając te umowy Organizacja ma zawsze na względzie, aby obejmowały one deklarację o zachowanie poufności.

2.7.4. Relacje z dostawcami

Organizacja zapewnia, ze wszystkie procesy związane z dostawcami, prowadzone są w sposób nadzorowany i kontrolowany gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa. Celem takiego postępowania jest zapewnienie ochrony aktywów organizacji, które są dostępne dla dostawców

Na to zapewnienie składa się:

- Uwzględniane w umowach lub porozumieniach wymagań dotyczących zachowania przez dostawców zasad bezpieczeństwa informacji
- Monitorowanie i przegląd usług dostawców

2.8. Bezpieczna konfiguracja i obsługa urządzeń końcowych

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 Najwyższe Kierownictwo.

2.8.1. Zasady korzystania z systemów informatycznych

Działania zdefiniowane w procedurach: PBI - 06 Korzystanie z zasobów informatycznych przez użytkowników oraz PBI - 07 Korzystanie z zasobów - administratorzy .

2.8.2. Oprogramowanie

Oprogramowanie jest instalowane wyłącznie przez Administratora systemu. Zabrania się instalowania jakiegokolwiek oprogramowania przez użytkowników. Oprogramowanie instalowane na komputerach jest legalne, niedopuszczalne jest instalowanie nawet tymczasowe nielegalnych wersji oprogramowania. Oprogramowanie może być wykorzystywane tylko i wyłącznie do użytku służbowego.

2.8.3. Poczta elektroniczna

Jeżeli Użytkownik korzysta z firmowego konta pocztowego (email), to może je wykorzystywać tylko i wyłącznie do użytku służbowego. Wszelka wpływająca korespondencja prywatna musi zostać natychmiast usunięta. Zasady korzystania z poczty elektronicznej opisane są w PBI - 06 Korzystanie z zasobów informatycznych przez użytkowników.

2.8.4. Procedura wykonywania przeglądów i konserwacji systemu

Sprzęt komputerowy definiowany jest, jako komputer stacjonarny, monitor oraz wszelkie komponenty wykorzystywane do jego obsługi (np. myszka, klawiatura)

Sprzęt mobilny definiowany jest, jako komputer mobilny typu laptop, tablet, telefon komórkowy, inny sprzęt elektroniczny o charakterze mobilnym.

Inne urządzenia elektryczne definiowane są jako wszelkie inne urządzenia wykorzystywane w celach służbowych niezależnie od sposobu oraz charakteru jego wykorzystania.

2.8.5. Sprzęt komputerowy

Każdy pracownik zobowiązany jest konserwować sprzęt komputerowy, na którym pracował w ostatnim okresie (czasie dłuższym niż miesiąc). Konserwacji okresowej należy dokonywać, co najmniej raz w miesiącu w następującym zakresie:

- wycieranie kurzu i zanieczyszczeń z obudowy komputera

- wycieranie kurzu i zanieczyszczeń z monitora

- czyszczenie klawiatury, myszki i innych komponentów sprzętu komputerowego z wszelkich zanieczyszczeń

Ponadto każdy użytkownik sprzętu komputerowego zobowiązany jest do natychmiastowego działania mającego na celu ochronę sprzętu przed awarią w przypadku wystąpienia zdarzenia mogącego wpłynąć na funkcjonalność i integralność sprzętu:

- kontakt z cieczą (np. wylanie herbaty na klawiaturę/obudowę komputera)

- kontakt z pożywieniem

- mechaniczne uszkodzenie/ naruszenie integralności sprzętu komputerowego

- inne nagłe przypadki mające wpływ na integralność oraz funkcjonalność sprzętu

W celu zapobiegnięciu wystąpienia przypadków mogących bezpośrednio wpłynąć na funkcjonalność sprzętu zabrania się spożywania wszelkich posiłków podczas użytkowania sprzętu komputerowego. Każdy pracownik zobowiązany jest do okresowej konserwacji powierzonego mu sprzętu mobilnego. Konserwacji należy dokonywać w zależności od stopnia wykorzystywania sprzętu jednak nie rzadziej, niż raz na trzy miesiące.

Każdy pracownik zobowiązany jest do konserwacji powierzonego mu sprzętu mobilnego typu telefon komórkowy. Konserwacji należy dokonywać w zależności od stopnia wykorzystania, jednak nie rzadziej niż raz na trzy miesiące. Zakres konserwacji obejmuje:

- czyszczenie obudowy i ekranu sprzętu z wszelkich zanieczyszczeń

Ponadto każdy pracownik jest zobowiązany do działania mającego na celu ochronę sprzętu mobilnego przed awarią w nagłych przypadkach przewidzianych w tożsamym punkcie dotyczącym sprzętu komputerowego.

2.9. Bezpieczeństwo zasobów ludzkich kompetencje, szkolenia i świadomość pracowników.

Organizacja 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.

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.

Zasoby ludzkie są ważnym czynnikiem analizowanym podczas przeprowadzania okresowej analizy ryzyka. Tylko kompetentni i zaufani pracownicy są gwarantem dostarczenia Klientom usług o odpowiednim poziomie jakości i bezpieczeństwa.

Najwyższe Kierownictwo podejmuje działania mające na celu podnoszenie świadomości dotyczącej bezpieczeństwa informacji wśród pracowników. Działania te przejawiają się w publikowaniu materiałów informacyjnych, informowaniu o zmianach i potrzebach SZBI.

Organizacja zarządza również bezpieczeństwem pracowników poprzez dobór i przeszkolenie kluczowego personelu pod kątem możliwości realizacji prac zastępczych na wypadek nieprzewidzianych sytuacji.

2.10. Bezpieczeństwo sieci

Organizacja 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
- opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy.
- kontrolowaniu wprowadzania wszelkich 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.

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

2.11. Zarządzanie incydentami związanymi z bezpieczeństwem informacji

W przypadku wszelkich incydentów w Organizacji powiadamiany jest Pełnomocnik . 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.

Szczegółowy opis postępowania z incydentami zawiera procedura PBI-03 „Zarządzanie Incydentami Bezpieczeństwa ”

2.12. Kopia zapasowa

Zasadniczym celem wykonywania kopii zapasowych jest zabezpieczenie danych przed utratą wynikłą z awarii sprzętu lub niewłaściwego użycia (skasowanie, niewłaściwa zmiana zawartości).

Kopie zapasowe są tworzone codziennie i okresowo testowane. Kopiom podlegają dane w systemach oraz w zasobach chmurowych.

2.13. Korzystanie z zabezpieczeń Kryptograficznych, zarządzanie kluczami

Organizacja zarządza zabezpieczeniami kryptograficznymi. Celem takiego postępowania jest zapewnienie bezpieczeństwa danych przetwarzanych w chmurze.

Skuteczna realizacja postawionego celu możliwa jest dzięki odpowiednim zapisom w umowach i polityce zarządzania kluczami.

W ramach stosowanych rozwiązań w chmurze, szyfrowanie jest używane podczas eksportu danych z programów do serwerów w sieci, za co odpowiada producent oprogramowania.

W przypadku pojawienia się konieczności stosowania takich zabezpieczeń Organizacja uwzględni to w analizie ryzyka i podejmie odpowiednie działania.

W organizacji kluczami licencyjnymi oraz zabezpieczającymi zarządza Administrator systemu w porozumieniu z Kierownikiem Placówki.

2.14. Klasyfikacja i przetwarzanie 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. Działania opisane w procedurze PBI - 08 Klasyfikacja informacji.

2.15. Zarządzanie lukami technicznymi

Organizacja 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. Pełnomocnik dba o ich aktualność i testuje je pod względem przydatności w sytuacji realnego zagrożenia. Powyższe zasady zapewniają, że Organizacja jest przygotowana na działanie również w przypadkach odbiegających od normy.

2.15.1. Pomiar skuteczności zabezpieczeń

W Organizacji został określony sposób pomiaru skuteczności zabezpieczeń w postaci wyznaczonych mierników, przypisanych do poszczególnych grup zabezpieczeń. Szczegółowy wykaz mierników zawiera formularz „pomiar skuteczności zabezpieczeń”.

2.16 Bezpieczny rozwój - Zgodność

Organizacja 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 urządzeń technicznych oraz prowadzone są audity wewnętrzne funkcjonowania systemu.

Dla zapewnienia zgodnego z prawem działania firmy realizowane są następujące przedsięwzięcia:

Przepisy prawa są identyfikowane, aktualizowane i okresowo przeglądane (nie rzadziej niż raz w roku). Dostępny jest rejestr aktów prawnych.

Identyfikacja wymogów prawnych

Organizacja zidentyfikowała wymogi formalno-prawne odnoszące się do bezpieczeństwa informacji i usług w chmurze i sporządziła wykaz odpowiednich aktów prawnych i zobowiązań w oparciu o:

- zidentyfikowane ryzyka,
- wymogi określone w odpowiednich pozwoleniach i decyzjach,
- uwarunkowanie związane z kontekstem organizacji,
- akty prawne w zakresie ochrony danych osobowych,

Wymogi te są uaktualniane przez Pełnomocnika raz na rok lub w zależności od zmian w przepisach prawnych.

Pełna lista wymagań prawnych i innych znajduje się w „PBI - 02 Zał.04 Akty prawne SZBI.”

Sposób komunikowania się

Pracownik odpowiedzialny za aktualizacje wymogów prawnych na raz w roku przekazuje informacje o zmianach w przepisach prawnych poczta elektroniczną.

2.17 Bezpieczeństwo Chmury

Organizacja dba o bezpieczeństwo informacji przechowywanych w chmurze. Celem takiego postępowania jest zapewnienie dostępności, integralności i poufności danych swoich i swoich klientów. Do chmury dostęp mają jedynie pracownicy firmy . Dodatkowo zasoby są udostępniane wg. odpowiedzialności i uprawnienień danego pracownika.

Dbając o bezpieczeństwo danych w chmurze organizacja określiła:
- zasady dotyczące aktualizacji i łatania błędów
- zasady weryfikacji i wykrywania działania szkodliwego oprogramowania
- zasady i rodzaje uwierzytelniania w usługach
- zasady szyfrowania danych w chmurze
- zasady ochrony i zapewnienia dostępności zasobów w chmurze
- zasady monitorowania, rejestrowania i raportowania incydentów
- zasady bezpiecznego usuwania lub niszczenia danych

3. Postanowienia końcowe

Organizacja dba o zapoznanie 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 Najwyższe Kierownictwo.

Naruszenia świadome, bądź przypadkowe niniejszej Polityki Bezpieczeństwa (wraz z wszystkimi dokumentami wykonawczymi) powoduje skutki prawne zgodnie z Regulaminem

Pracy, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez sąd.

W ramach doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji deklarowana jest wola współpracy w zakresie poprawy stanu ochrony aktywów informacyjnych z:

- Organizacjami certyfikującymi na zgodność ze standardami bezpieczeństwa, w tym na zgodność z normą ISO/IEC 27001:2022
- Ekspertami w zakresie bezpieczeństwa
- oraz pozostałymi instytucjami (Klientami, Dostawcami, Partnerami i innymi zainteresowanymi stronami)

4 Dokumenty związane

Brak

5 Załączniki

brak

Data	Nr wersji procedury	Opis wprowadzonej zmiany w odniesieniu do poprzedniej wersji