PKJBI

Program Kontroli Jakości Bezpieczeństwa Informacji

W. 2020 r.

Spis treści:

Rozdział I:

Terminy i definicje

W niniejszym dokumencie zastosowano następujące terminy i definicje:

Aktywa informacyjne - wszystko, co ma wartość dla organizacji z uwagi na zawarte w nim informacje

Właściciel aktywa – osoba w strukturze organizacyjnej np. kierownik działu, która ma formalnie zatwierdzoną kierowniczą odpowiedzialność za nadzorowanie, rozwój, utrzymanie, korzystanie i bezpieczeństwo aktywów.

Dostępność - właściwość polegająca na tym, że informacja jest dostępna i użyteczna na żądanie upoważnionej osoby, firmy zewnętrznej lub innej strony trzeciej.

Poufność - właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, firmom zewnętrznym lub innym stronom trzecim.

Integralność – właściwość polegająca na tym że informacja nie została zmieniona, dodana lub usunięta w nieautoryzowany sposób.

Bezpieczeństwo informacji - zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność

Zdarzenie związane z bezpieczeństwem informacji - określony stan, 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 - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji

System Zarządzania Bezpieczeństwem Informacji (SZBI) - część całościowego systemu zarządzania, wynikająca z analizy ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia metod i zasad działania firmy badawczej oraz odpowiedniego planowania przyszłych działań i zasobów zapewniających bezpieczeństwo informacji.

Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez kierownictwo firmy badawczej, odpowiedzialna za wdrożenie i utrzymywanie SZBI, w szczególności nadzorująca przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę informacji w sposób odpowiedni do zagrożeń

Ryzyko szczątkowe - ryzyko pozostające po procesie postępowania z ryzykiem

Analiza ryzyka - systematyczne wykorzystywanie informacji do zidentyfikowania źródeł zagrożeń i oszacowania ryzyka

Szacowanie ryzyka - całościowy proces analizy i oceny ryzyka

Ocena ryzyka - proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka

Zarządzanie ryzykiem - skoordynowane działania kierowania i zarządzania organizacją z uwzględnieniem wyników analizy ryzyka

Postępowanie z ryzykiem - proces wyboru i wdrażania środków modyfikujących ryzyko

Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Pseudonimizacja - dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, Stosowanie pseudonimizacji powinno zapewnić, że możliwe sposoby nieuzasadnionego

zidentyfikowania danej osoby, są mało prawdopodobne biorąc pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania oraz uwzględniając technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny.
Anonimizacja - oznacza takie przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów i sił.
Kodeks Postępowania – oznacza Kodeks Postępowania Dotyczący Przetwarzania Danych Osobowych Przez Agencje Badawcze.

Rozdział II
Stosowanie podstawowych zabezpieczeń

Niezależnie od wymienionych poniżej zabezpieczeń firma badawcza powinna wprowadzić wszystkie możliwe inne zabezpieczenia, które są konieczne aby ograniczyć ryzyko zidentyfikowane zgodnie z przyjętą metodą szacowania ryzyka.

2.1 Organizacja bezpieczeństwa informacji

2.1.1 Kierownictwo powinno aktywnie wspierać bezpieczeństwo informacji w całej organizacji poprzez wskazanie wyraźnego kierunku działania, demonstrowanie zaangażowania, wyznaczenie IOD posiadającego jednoznaczne przypisanie uprawnień i przyjmowanie odpowiedzialności w zakresie bezpieczeństwa informacji.

2.1.2 Działania w zakresie bezpieczeństwa informacji powinny być koordynowane przez reprezentantów różnych części organizacji pełniących odpowiednie role i funkcje.

2.1.3 Wszelka odpowiedzialność związana z bezpieczeństwem informacji powinna być wyraźnie zdefiniowana.

2.1.4 Powinien zostać zdefiniowany i wdrożony proces autoryzacji przez kierownictwo nowych środków służących do przetwarzania informacji.

2.1.5 Wymagania dotyczące umów o zachowaniu poufności i nieujawnianiu informacji odzwierciedlające potrzeby firmy badawczej w zakresie ochrony informacji powinny być określone i regularnie przeglądane.

2.1.6 Powinno się utrzymywać odpowiednie kontakty z właściwymi organami władzy, w zakresie określonym obowiązującymi przepisami prawa. Należy także, w celu zapewnienia odpowiedniego poziomu wiedzy technicznej, utrzymywać kontakty z oraz stronami zainteresowanymi bezpieczeństwem, specjalistycznymi forami związanymi z bezpieczeństwem oraz profesjonalnymi stowarzyszeniami.

2.1.7 Podejście do zarządzania bezpieczeństwem informacji oraz jego realizacja (zabezpieczenia, polityki, procesy i procedury bezpieczeństwa informacji) powinny być poddawane niezależnym przeglądom w zaplanowanych odstępach czasu, nie rzadziej niż raz do roku lub wtedy, kiedy nastąpiły w nich znaczące zmiany.

2.1.8 Kierownicy powinni zapewnić, że wszystkie procedury bezpieczeństwa obszaru, za który są odpowiedzialni, są wykonywane prawidłowo, tak aby osiągnąć zgodność z politykami bezpieczeństwa i normami.

2.1.9 Aby minimalizować ryzyko zakłóceń procesów biznesowych należy starannie planować i uzgadniać wymagania audytu oraz działań związanych ze sprawdzeniem eksploatowanych systemów.

2.1.10 Dostęp do narzędzi audytu systemów informacyjnych powinien być chroniony, aby zapobiec nadużyciom lub naruszeniu bezpieczeństwa.

2.2 Współpraca z firmami zewnętrznymi, w tym z klientami, ośrodkami regionalnymi lub ankieterami prowadzącymi działalność gospodarczą

2.2.1 Ryzyka informacji należącej do firmy badawczej i środków przetwarzania informacji, związane z firmami zewnętrznymi, należy zidentyfikować przed podpisaniem umowy o współpracy. W przypadku umów, które weszły w życie przed opublikowaniem niniejszej wersji standardu, przeglądu należy dokonać przed przyznaniem dostępu tym firmom.

2.2.2 Wszystkie zidentyfikowane zabezpieczenia powinny być wprowadzanie przed przyznaniem klientom dostępu do informacji lub aktywów firmy badawczej.

2.2.3 Umowy z firmami zewnętrznymi dotyczące dostępu, przetwarzania, przekazywania lub zarządzania informacjami firmy badawczej lub środkami przetwarzania informacji, lub dodanie produktów lub usług obejmujących dostęp do środków przetwarzania informacji, powinny obejmować wszystkie stosowne wymagania bezpieczeństwa oraz w stosownych przypadkach wypełniać elementy istotne tzw. Umowy Powierzenia Przetwarzania zgodnej z art. 28 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r (ogólne rozporządzenie o ochronie danych). Należy zdefiniować minimalny wymagany poziom zabezpieczeń i bezpieczeństwa jaki strona trzecia musi spełnić przed przekazaniem jej dostępu do informacji.

2.2.4 Role i odpowiedzialności pracowników, wykonawców oraz użytkowników reprezentujących firmy zewnętrzne z zakresu bezpieczeństwa informacji powinny być określone i udokumentowane.

2.2.5 W przypadku umów serwisowych z zewnętrznymi firmami informatycznymi należy zapewnić, że zabezpieczenia, definicje usług oraz poziomy dostaw zawarte w umowach serwisowych są wdrożone, wykonywane i utrzymywane przez firmy serwisujące. Należy ocenić wpływ usługi na bezpieczeństwo informacji przed rozpoczęciem świadczenia usług.

2.2.6 Usługi, raporty i zapisy dostarczane przez zewnętrzne firmy, w tym obejmujące serwis IT, powinny być regularnie monitorowane i przeglądane oraz regularnie audytowane.

2.2.7 Zmiany w zakresie usług dostarczanych przez firmy zewnętrzne, łącznie z utrzymaniem i doskonaleniem istniejących polityk bezpieczeństwa, procedur i zabezpieczeń, powinny być zarządzane z uwzględnieniem krytyczności związanych z tym systemów i procesów biznesowych oraz wymogiem ponownego szacowania ryzyk.

2.3 Ochrona aktywów informacyjnych firmy badawczej oraz klasyfikowanie informacji

2.3.1 Wszystkie aktywa informacyjne powinny być jasno zidentyfikowane, należy sporządzić i utrzymywać rejestr wszystkich ważnych aktywów.

2.3.2 Wszystkie informacje i aktywa związane ze środkami przetwarzania informacji powinny mieć przypisanego właściciela.

2.3.3 Zasady dopuszczalnego korzystania z informacji oraz aktywów związanych ze środkami przetwarzania informacji powinny być określone, udokumentowane i wdrożone.

2.3.4 Informacje powinny być klasyfikowane z uwzględnieniem ich wartości, wymagań prawnych, wrażliwości i krytyczności dla organizacji oraz (w przypadku danych osobowych) osób, których dane są przetwarzane.

2.3.5 Odpowiedni zbiór procedur do oznaczania informacji i postępowania z nimi, należy opracować i wdrożyć według przyjętego w organizacji schematu klasyfikacji informacji.

2.4 Nadzór nad pracownikami, wykonawcami i osobami reprezentującymi

2.4.1 Należy przeprowadzić weryfikację wszystkich kandydatów do zatrudnienia w firmie badawczej, wykonawców oraz użytkowników reprezentujących firmy zewnętrzne, w tym ośrodki regionalne, zgodnie z odpowiednimi przepisami prawa, regulacjami wewnętrznymi i etyką oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, która ma być udostępniona, oraz zidentyfikowanych ryzyk.

2.4.2 Uzgodnienie i podpisanie zasad i warunków umowy zatrudnienia powinno być częścią zobowiązań kontraktowych pracowników, wykonawców oraz użytkowników reprezentujących firmy zewnętrzne, w tym ośrodki regionalne, precyzującej ich obowiązki oraz obowiązki firmy badawczej w zakresie bezpieczeństwa.

2.4.3 Wszyscy pracownicy firmy badawczej oraz, tam gdzie jest to wskazane, wykonawcy i użytkownicy reprezentujący firmy zewnętrzne, w tym ośrodki regionalne, powinni zostać odpowiednio przeszkoleni, oraz powinni być regularnie informowani o uaktualnieniach polityk i procedur obowiązujących w organizacji, które są związane z wykonywaną przez nich pracą.

2.4.4 Wobec pracowników, którzy naruszyli bezpieczeństwo powinien być wdrożony formalny, proporcjonalny do wagi incydentu, proces postępowania dyscyplinującego.

2.4.5 Odpowiedzialność związaną z zakończeniem lub zmianą zatrudnienia należy jasno określić i przypisać.

2.4.6 Wszyscy pracownicy, wykonawcy i użytkownicy reprezentujący firmy zewnętrzne powinni być zobowiązani do zwrotu wszystkich posiadanych aktywów informacyjnych firmy badawczej w momencie zakończenia stosunku pracy, kontraktu lub umowy.

2.4.7 Prawa dostępu pracowników, wykonawców, użytkowników reprezentujących firmy zewnętrzne do informacji i środków przetwarzania informacji, należy odebrać, w momencie zakończenia stosunku pracy, kontraktu lub umowy, lub zmodyfikować zgodnie z zaistniałymi zmianami zatrudnienia.

2.5 Bezpieczeństwo fizyczne i środowiskowe

2.5.1 Należy identyfikować i definiować zagrożenia związane z dostępem fizycznym oraz zagrożenia środowiskowe

2.5.2 Jeżeli to jest uzasadnione, należy wydzielić obszary o różnym stopniu dostępności (serwerownie, archiwa, działy badawcze).

2.5.3 Granice obszaru bezpiecznego (bariery takie jak ściany, bramki wejściowe na kartę lub recepcja z obsługą) powinny być stosowane w celu ochrony obszarów zawierających informacje i środki przetwarzania informacji.

2.5.4 Obszary bezpieczne powinny być chronione przez odpowiednie fizyczne zabezpieczenia wejścia, zapewniające, że tylko autoryzowany personel ma przyznane prawa dostępu.

2.5.5 Należy zaprojektować i stosować ochronę fizyczną biur, w tym pomieszczeń biurowych, powierzchni współużytkowanych i urządzeń.

2.5.6 Należy, z uwzględnieniem ryzyka wystąpienia każdego ze zdarzeń, opracować i stosować ochronę fizyczną i środowiskową przed zniszczeniami spowodowanymi przez pożar, zalanie, trzęsienie ziemi, wybuch, niepokoje społeczne i inne formy naturalnych lub spowodowanych przez człowieka katastrof.

2.5.7 Należy opracować i stosować mechanizmy ochrony fizycznej oraz wytyczne do pracy w obszarach bezpiecznych.

2.5.8 Punkty dostępu, przez które nieuprawnione osoby mogą wejść do obszaru bezpiecznego należy nadzorować i, jeśli to możliwe, odizolować od środków przetwarzania informacji w celu uniknięcia nieautoryzowanego dostępu.

2.5.9 Sprzęt służący przetwarzaniu informacji należy rozlokować i chronić w taki sposób, aby redukować ryzyka wynikające z zagrożeń środowiskowych oraz możliwości nieautoryzowanego dostępu.

2.5.10 Sprzęt służący przetwarzaniu informacji należy chronić przed awariami zasilania lub zakłóceniami spowodowanymi awariami systemów wspomagających.

2.5.11 Okablowanie zasilające i telekomunikacyjne służące do przesyłania danych lub wspomagające usługi informacyjne należy chronić przed nieuprawnionym dostępem.

2.5.12 Sprzęt służący przetwarzaniu informacji należy prawidłowo konserwować, aby zapewnić jego ciągłą dostępność i integralność.

2.5.13 Sprzęt służący przetwarzaniu informacji, informacje lub oprogramowanie nie powinny być wynoszone poza organizację bez uprzedniego zezwolenia.

2.5.14 Sprzęt służący przetwarzaniu informacji wykorzystywany lub pozostający poza siedzibą firmy badawczej należy chronić przy uwzględnieniu ryzyk związanych z pracą poza obszarem chronionym.

2.6 Zarządzanie systemami i sieciami IT

2.6.1 Procedury eksploatacyjne powinny być udokumentowane, utrzymywane i dostępne dla wszystkich użytkowników, którzy ich potrzebują.
2.6.2 Zmiany w środkach przetwarzania informacji i systemach powinny być kontrolowane.
2.6.3 Należy rozdzielić obowiązki i zakresy odpowiedzialności w celu ograniczenia możliwości nieuprawnionej lub nieumyślnej modyfikacji lub niewłaściwego użycia aktywów informacyjnych firmy badawczej.
2.6.4 Należy oddzielić urządzenia rozwojowe, testowe i eksploatacyjne, aby zredukować ryzyko nieupoważnionego dostępu lub zmian w systemach eksploatacyjnych.
2.6.5 Wykorzystanie zasobów służących przetwarzaniu informacji należy monitorować i regulować oraz przewidywać przyszłą pojemności systemów, aby zapewnić ich właściwą wydajność.
2.6.6 Należy opracować kryteria odbioru nowych systemów informacyjnych przed ich odbiorem. Dotyczy to również uaktualnień i nowych wersji oraz odpowiednich testów systemów prowadzonych w fazie rozwojowej.
2.6.7 Należy wdrożyć zabezpieczenia zapobiegające, wykrywające i usuwające kod złośliwy oraz właściwe procedury uświadamiania użytkowników.
2.6.8 Kopie zapasowe informacji i oprogramowania powinny być regularnie tworzone i testowane zgodnie z ustaloną polityką wykonywania kopii zapasowych.
2.6.9 Sieci powinny być odpowiednio zarządzanie i nadzorowanie, aby ochronić je przed zagrożeniami i utrzymywać bezpieczeństwo systemów i aplikacji sieciowych, w tym przesyłania informacji.

2.7 Zapewnienie bezpieczeństwa przy przekazywaniu informacji

2.7.1 Należy wdrożyć formalne polityki wymiany informacji, procedury i zabezpieczenia w celu ochrony wymiany informacji przekazywanej przy użyciu wszystkich rodzajów środków komunikacji.
2.7.2 Nośniki zawierające informacje powinny być chronione przed nieautoryzowanym dostępem, niewłaściwym użyciem lub uszkodzeniem podczas transportu poza fizyczne granice firmy badawczej.
2.7.3 Informacje zawarte w wiadomościach elektronicznych powinny być odpowiednio zabezpieczone.
2.7.4 Należy opracować i wdrożyć polityki i procedury dla ochrony informacji związanej z połączeniami między biznesowymi systemami informacyjnymi.
2.7.5 Należy wdrożyć procedury zarządzania nośnikami wymiennymi. Nośniki, które nie będą już dłużej wykorzystywane, powinny być bezpiecznie niszczone, zgodnie z formalnymi procedurami.
2.7.6 Należy wdrożyć procedury postępowania z informacjami oraz ich przechowywania na nośnikach, w celu ochrony informacji przed nieautoryzowanym ujawnieniem lub niewłaściwym użyciem.

2.8 Monitorowanie nieautoryzowanych działań związanych z przetwarzaniem informacji

2.8.1 Dzienniki audytu rejestrujące działania użytkowników oraz zdarzenia związane z bezpieczeństwem informacji powinny być tworzone i przechowywane przez określony czas, na potrzeby przyszłych postępowań wyjaśniających oraz monitorowania kontroli dostępu.
2.8.2 Należy wdrożyć procedury monitorowania użycia środków przetwarzania informacji, a wyniki działań monitorujących należy regularnie przeglądać.
2.8.3 Podsystemy logowania oraz informacje zawarte w dziennikach powinny być chronione przed manipulacją i nieautoryzowanym dostępem.
2.8.4 Działania administratorów i operatorów systemów powinny być rejestrowane. Błędy należy rejestrować i analizować i podjąć odpowiednie działania.
2.8.5 Zegary wszystkich stosownych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa, powinny być synchronizowane z uzgodnionym, dokładnym źródłem czasu.

2.9 Zarządzanie dostępem do systemów IT

2.9.1 Polityka kontroli dostępu powinna być ustanowiona, udokumentowana i poddawana przeglądom na podstawie potrzeb biznesowych i wymagań bezpieczeństwa.

2.9.2 Przyznawanie i odbieranie dostępu do wszystkich systemów i usług informacyjnych powinno opierać się na formalnej procedurze rejestrowania i wyrejestrowywania użytkowników. Należy ograniczyć i kontrolować przyznawanie i korzystanie z przywilejów.

2.9.3 Przydzielanie haseł powinno być kontrolowane za pośrednictwem formalnego procesu zarządzania.

2.9.4 Kierownictwo powinno dokonywać regularnych przeglądów praw użytkowników na podstawie formalnego procesu.

2.9.5 Podczas wyboru i używania haseł użytkownicy powinni postępować zgodnie ze sprawdzonymi praktykami bezpieczeństwa. Złożoność i powtarzalność haseł powinna być narzucona, okres wymiany hasła nie powinien przekraczać 90 dni.

2.9.6 Użytkownicy powinni zapewnić odpowiednią ochronę sprzętu pozostawionego bez opieki (zamykanie sesji, aplikacji, blokowanie dostępu do systemu, wyłączanie laptopów na czas podróży)

2.9.7 Należy wprowadzić politykę czystego biurka dla dokumentów papierowych i nośników, a dla środków przetwarzania informacji – politykę czystego ekranu.

2.9.8 Przy dostępie zdalnych użytkowników należy stosować odpowiednie metody uwierzytelniania.

2.9.9 Fizyczny i logiczny dostęp do urządzeń przetwarzających informacje w celach diagnostycznych i konfiguracyjnych powinien być kontrolowany i nadzorowany. Dotyczy to zarówno serwerów, aplikacji, baz danych jak też urządzeń sieciowych.

2.9.10 We współużytkowanych sieciach, szczególnie tych, które wykraczają poza granice organizacji, powinno się ograniczyć możliwość podłączania się użytkowników, zgodnie z polityką kontroli dostępu oraz wymaganiami aplikacji biznesowych.

2.9.11 Należy wdrożyć kontrolę routingu w sieciach, aby zapewnić, że połączenia pomiędzy komputerami i przepływ informacji nie naruszają polityki dostępu do aplikacji biznesowych.

2.9.12 Należy zdefiniować procedury dostępu dla administratorów do systemów operacyjnych, baz danych i aplikacji oraz urządzeń sieciowych. Należy uwzględnić i zdefiniować sposób postępowania z kontami generycznymi (konta dostępne default – administracyjne, testowe, szkoleniowe).

2.9.13 Wszyscy użytkownicy powinni mieć unikalne identyfikatory (ID użytkownika) do swojego osobistego i wyłącznego użytku oraz należy zastosować odpowiednią technikę uwierzytelnienia do sprawdzenia deklarowanej tożsamości użytkownika.

2.9.14 Dostęp użytkowników i personelu obsługi technicznej do informacji oraz funkcji aplikacji powinien być ograniczony, zgodnie ze zdefiniowaną polityką dostępu.

2.9.15 Należy wprowadzić formalną politykę oraz zastosować odpowiednie zabezpieczenia w celu ochrony przed ryzykiem wynikającym z użycia przetwarzania mobilnego i środków komunikacji mobilnej.

2.9.16 Należy opracować i wdrożyć politykę, plany operacyjne i procedury dla czynności wykonywanych w ramach pracy na odległość.

2.10 Rozwój infrastruktury IT

2.10.1 Deklaracje wymagań biznesowych dotyczących nowych systemów lub rozszerzeń dla istniejących systemów powinny zawierać wymagania dotyczące zabezpieczeń.

2.10.2 Należy wprowadzić procedury kontroli instalacji oprogramowania w eksploatowanych systemach. Dostęp do kodów źródłowych powinien być ograniczony.

2.10.3 Należy nadzorować wprowadzanie zmian w infrastrukturze IT za pomocą formalnych procedur kontroli zmian.

2.10.4 Po dokonaniu zmian w systemach operacyjnych należy przeprowadzić przegląd krytycznych aplikacji biznesowych i przetestować je tak, aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji lub bezpieczeństwo.

2.10.5 Zmiany w oprogramowaniu powinny być minimalne, ograniczone do zmian niezbędnych, a wszelkie zmiany powinny być ściśle nadzorowane.

2.10.6 Organizacja powinna nadzorować i monitorować prace rozwojowe nad oprogramowaniem powierzone firmie zewnętrznej.

2.11 Zarządzanie incydentami związanymi z bezpieczeństwem informacji

2.11.1 Zdarzenia związane z bezpieczeństwem informacji powinny być zgłaszane i rejestrowane poprzez odpowiednie kanały organizacyjne tak szybko, jak to możliwe lecz bez zbędnej zwłoki do wiadomości IOD lub osób przez niego wyznaczonych.

2.11.2 Wszystkich pracowników, wykonawców i użytkowników reprezentujących firmy zewnętrzne, w tym ośrodki regionalne, korzystających z systemów informacyjnych i usług, należy zobowiązać do zgłaszania zaobserwowanych lub podejrzewanych słabości bezpieczeństwa w systemach lub usługach.

2.11.3 Należy wprowadzić odpowiedzialność kierownictwa oraz procedury zapewniające szybką, skuteczną i uporządkowaną reakcję na incydenty związane z bezpieczeństwem informacji.

2.11.4 Jeśli działania podejmowane po wystąpieniu incydentu związanego z bezpieczeństwem informacji obejmują kroki prawne (natury cywilnoprawnej, karnej lub administracyjnej), powinno się zabezpieczyć materiał dowodowy w celu dochodzenia roszczeń, lub ochrony dóbr prawnych. Takie same działania należy podjąć gdy kroki prawne związane z incydentem podejmowane są przeciwko firmie badawczej.

2.12 Zapewnienie zgodności z wymaganiami prawnymi

2.12.1 Wszelkie wymagania wynikające z zarządzeń i umów oraz podejście do ich wypełniania powinny być zgodne z obowiązującym w Polsce prawem. Ponadto wdrożone wymagania powinny być wyraźnie określone, udokumentowane i aktualizowane dla każdego systemu informacyjnego i bazy danych w firmie badawczej.

2.12.2 Należy chronić wszelkie informacje, w tym dane osobowe przed utratą, zniszczeniem lub sfałszowaniem zgodnie z wymaganiami ustawowymi, regulacjami wewnętrznymi oraz wymaganiami biznesowymi i kontraktowymi.

2.12.3 Należy zapewnić w regulacjach wewnętrznych i w umowach zgodność ochrony danych osobowych i prywatności z odpowiednimi przepisami prawa..

2.12.4 Używanie zabezpieczeń kryptograficznych powinno być zgodnie z odpowiednimi umowami, prawem i regulacjami wewnętrznymi.

Rozdział III

Wymagania dotyczące Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

3.1 Ustanowienie Polityki Bezpieczeństwa Informacji

Firma badawcza powinna zdefiniować politykę bezpieczeństwa informacji, w szczególności w zakresie wymagań podstawowych zawartych w rozdziale II oraz uwzględniającą charakterystykę prowadzonych projektów badawczych i innej działalności, wewnętrznej organizacji, jej lokalizacji, aktywów i technologii, która:

a) wyznacza metody i zasady działania oraz role i odpowiedzialności w zakresie zapewnienia bezpieczeństwa informacji
b) stanowi podstawę do ustalania celów dotyczących bezpieczeństwa informacji oraz planowania zasobów zapewniających bezpieczeństwo informacji;
c) bierze pod uwagę wymagania biznesowe oraz prawne lub o charakterze regulacyjnym, a także zobowiązania związane z bezpieczeństwem wynikające z umów;

d) określa kryteria i metody według których ma być oceniane ryzyko związane z bezpieczeństwem informacji i ochroną danych osobowych.

Polityka bezpieczeństwa informacji powinna zostać udokumentowana, zatwierdzona przez kierownictwo, opublikowana i podana do wiadomości wszystkim pracownikom i właściwym stronom zewnętrznym.

Polityka bezpieczeństwa powinna być poddawana regularnemu przeglądowi, a w przypadku istotnych zmian powinna zapewniać, że pozostaje przydatna, adekwatna i skuteczna.

3.2 Zarządzanie ryzykiem

Firma badawcza w ramach zarządzania ryzykiem związanym z bezpieczeństwem informacji powinna:

a) Wdrożyć metodę szacowania ryzyka zapewniającą odpowiednie zdefiniowanie bezpieczeństwa informacji w kontekście prowadzonej działalności, wpływu zidentyfikowanych ryzyk na osoby, których dane są przetwarzane, a także uwzględnienie obowiązujących wymagań prawnych i nadzoru.
b) Opracować kryteriów akceptacji ryzyka i określić akceptowalny poziom ryzyka.
c) Zidentyfikować zagrożenia dotyczące bezpieczeństwa informacji, w szczególności:
    1) zidentyfikować aktywa znajdujące się w zakresie SZBI oraz właścicieli tych aktywów. Patrz wyżej
    2) określić zagrożenia dla tych aktywów.
    3) ustalić podatności, które mogą powodować zagrożenia.
    4) określić możliwe skutki utraty poufności, integralności i dostępności w odniesieniu do aktywów, w tym skutki dla osób, których dane są przetwarzane.
d) Analizować i oceniać ryzyka, w szczególności:
    1) oszacować szkody i straty biznesowe, które mogą wyniknąć z naruszenia bezpieczeństwa, biorąc pod uwagę potencjalne konsekwencje utraty poufności, integralności i dostępności aktywów.
    2) oszacować skutki dla osób, których dane są przetwarzane, a które mogą wyniknąć z naruszenia bezpieczeństwa informacji będących danymi osobowymi, biorąc pod uwagę potencjalne konsekwencje utraty poufności, integralności i dostępności aktywów.
    3) oszacować realne prawdopodobieństwo zdarzenia się takiego naruszenia bezpieczeństwa w świetle istotnych zagrożeń i podatności oraz konsekwencji związanych z tymi aktywami oraz aktualnie wdrożonymi zabezpieczeniami.
    4) wyznaczyć poziomy ryzyk.
    5) stosując kryteria akceptacji ryzyk stwierdzić, czy ryzyko jest akceptowalne, czy też wymaga postępowania z ryzykiem.
e) Zidentyfikować i ocenić warianty postępowania z ryzykiem, wprowadzić odpowiednie i możliwe do zastosowania działania, które mogą obejmować:
    1) zastosowanie odpowiednich zabezpieczeń;
    2) poznanie i zaakceptowanie ryzyk, w sposób świadomy i obiektywny, przy założeniu, że jasno spełniają warunki wyznaczone w polityce organizacji oraz kryteria akceptowania ryzyk
    3) unikanie ryzyk, między innymi poprzez wprowadzenia zmian zasad i metod realizacji procesów biznesowych
    4) przeniesienie związanych ryzyk biznesowych na innych uczestników, np. ubezpieczycieli, dostawców lub inne strony trzecie.

3.3 Zarządzanie ciągłością działania

3.3.1 Analiza scenariuszy ryzyka utraty ciągłości działania

Firma badawcza powinna zidentyfikować zdarzenia, które mogą spowodować przerwanie procesów, łącznie z prawdopodobieństwem ich wystąpienia, wpływem na rezultaty biznesowe oraz konsekwencjami dla bezpieczeństwa informacji. Należy opisać kluczowe scenariusze ryzyk wywołane tymi zdarzeniami, które prowadzą do utraty ciągłości działania w ramach kluczowych procesów,

W przypadku każdego istotnego scenariusza ryzyka należy opracować i utrzymywać zarządzany proces zapewnienia ciągłości działania, który określa wymagania bezpieczeństwa informacji potrzebne do zapewnienia ciągłości działania organizacji.

3.3.2 Plany ciągłości działania

Należy opracować, udokumentować i wdrożyć plany utrzymania lub odtworzenia działalności, zapewniające dostępność informacji na wymaganym poziomie i w wymaganym czasie w przypadku wystąpienia kluczowych scenariuszy ryzyk w krytycznych procesach biznesowych.

Plany ciągłości działania powinny jednoznacznie określać zakresy zadań, uprawnień i odpowiedzialności za wykonanie planu dla każdego z kluczowych scenariuszy ryzyk.

Należy zachować jednolitą strukturę planów ciągłości działania, aby zapewnić, że plany dla wszystkich scenariuszy ryzyk oraz wymagania bezpieczeństwa informacji są ze sobą zgodne oraz w celu zidentyfikowania priorytetów testowania i utrzymania.

Należy regularne testować i uaktualniać plany ciągłości działania tak, aby zapewnić ich aktualność i skuteczność.

3.4 Ochrona danych osobowych

3.4.1 Wymagania podstawowe:

Kierownictwo firmy badawczej w ramach SZBI powinno zapewnić bezpieczeństwo danych osobowych w każdym przypadku ich przetwarzania, w szczególności poprzez formalne zobowiązanie IOD do wdrożenia w ramach SZBI odpowiednich rozwiązań organizacyjnych, procedur oraz określenie osób odpowiedzialnych za przetwarzanie danych osobowych.

W kwestiach dotyczących podstawowych wymagań ochrony danych osobowych stosuje się odpowiednio postanowienia Kodeksu Postępowania, w szczególności w zakresie:

a) spełnienia obowiązku informacyjnego w stosunku do osób, których dane są przetwarzane;
b) uzyskania dostępu do informacji o przetwarzaniu danych osobowych przez osoby, których dane są przetwarzane;
c) realizacji praw osób, których dane są przetwarzane;
d) retencji danych osobowych;
e) reagowania na naruszenia ochrony danych osobowych;
f) powierzenia przetwarzania danych osobowych.

IOD powinien uwzględnić stosowanie metod SZBI oraz wdrożenie wszelkich możliwych środków, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych polegających m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej anonimizacji lub pseudonimizacji danych osobowych, przejrzystości co do zasad przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń.

3.4.2 Procedury postępowania w przypadku projektów wymagających przetwarzania danych osobowych

Wszystkie projekty, w trakcie realizacji których konieczne jest przetwarzanie danych osobowych powinny być oznaczone w celu zapewnienia identyfikowalności oraz okresowej weryfikacji w ramach audytów bezpieczeństwa informacji oraz indywidualnej analizy ryzyka związanego z przetwarzaniem danych osobowych.

Procedury postępowania w przypadku realizacji takich „oznaczonych” projektów powinny obejmować co najmniej:

1. określenie i wprowadzenie do umowy o realizację projektu zasad zapewnienia bezpieczeństwa w przypadku otrzymania bazy danych od klienta lub innego partnera współpracującego, określenie w umowie odpowiedzialności i zasad postępowania w zależności od ryzyka związanego z przetwarzaniem danych osobowych
2. wprowadzenie do umowy adekwatnych do ryzyka zasad postępowania w przypadku udziału innych podmiotów w trakcie realizacji projektu, w tym koordynatorów prowadzących działalność gospodarczą, centrów telefonicznych i innych stron trzecich.
3. w przypadku stałej umowy o współpracy obowiązek regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych
4. w przypadku naruszenia ochrony danych osobowych stosuje się odpowiednio postanowienia punktu 10 Kodeksu Postępowania („Naruszenia ochrony Danych osobowych”).
5. obowiązek ustalenia i udokumentowania w dokumentacji projektowej minimalnego zakresu przetwarzania danych osobowych w celu zapewnienia odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.
6. umożliwienia dostępu do danych osobowych osobie zainteresowanej oraz możliwości składania wniosków w zakresie przetwarzania jej danych osobowych, w ramach procedury powinien być zaplanowany sposób weryfikacji tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów – w zakresie weryfikacji tożsamości osoby żądającej dostępu do danych osobowych stosuje się odpowiednio postanowienia uregulowane w punkcie 4.2.3 Kodeksu Postępowania.
7. sposób działania organizacji zapobiegający przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne. W szczególności powinien być ustalony termin usuwania danych osobowych lub okresowego przeglądu zgodnie z regulacjami Kodeksu Postepowania dotyczącymi retencji danych. Następne działania w przypadku wykrycia nieprawidłowości zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe.
8. w dokumentacji dostępnej respondentom - osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.

W dokumentacji każdego „oznaczonego” projektu należy przechowywać zapisy potwierdzające przeprowadzenie analizy ryzyka związanego z przetwarzaniem danych osobowych oraz realizację projektu zgodnie z wymaganiami odpowiednich wymagań SZBI i procedur postępowania.

3.5 Monitorowanie i przegląd SZBI

Firma badawcza powinna w ramach monitorowania i przeglądu SZBI:

a) Wykonywać przeglądy szacowania ryzyka w zaplanowanych odstępach czasu, biorąc pod uwagę zmiany:
   1) w organizacji;
   2) technologii;
   3) celów biznesowych i procesów;
   4) zidentyfikowanych zagrożeń;

5) skuteczności wdrożonych zabezpieczeń;
6) zewnętrznych zdarzeń, takich jak zmiany prawa lub stosownych regulacji, zmian wynikających z umów oraz zmian o charakterze społecznym.

b) Przeprowadzać wewnętrzne audyty bezpieczeństwa informacji w zaplanowanych odstępach czasu.
c) Uaktualniać stosowane zabezpieczenia, mając na uwadze wyniki monitorowania i przeglądu działalności.
d) Rejestrować działania i zdarzenia, które mogą mieć wpływ na skuteczność lub wydajność funkcjonowania SZBI
e) Kierownictwo firmy badawczej powinno przeprowadzać regularne przeglądy skuteczności SZBI (w tym zgodności z polityką i celami związanymi z zapewnieniem bezpieczeństwa informacji oraz przegląd zabezpieczeń), biorąc pod uwagę wyniki audytów bezpieczeństwa, postępowania w przypadku incydentów, rezultaty pomiarów skuteczności, sugestii oraz informacji zwrotnych od wszystkich zainteresowanych stron.

3.6 Wymagania dotyczące dokumentacji

Dokumentacja SZBI powinna zapewnić, że działania są zgodne z decyzjami kierownictwa i politykami oraz że zapisy rezultatów działań są odtwarzalne.

Dokumentacja SZBI powinna obejmować:

a) udokumentowane deklaracje polityki bezpieczeństwa informacji i cele w tym zakresie;
b) opis metody szacowania ryzyka;
c) plan postępowania z ryzykiem;
d) udokumentowane polityki i procedury potrzebne firmie badawczej do zapewnienia skutecznego planowania, eksploatacji i sterowania procesami bezpieczeństwa informacji i opis pomiaru skuteczności zabezpieczeń;

UWAGA 1: Tam, gdzie pojawia się termin “udokumentowana polityka lub procedura”, oznacza to, że procedura jest zdefiniowana, udokumentowana, wdrożona (zatwierdzona formalnie przez kierownictwo lub uprawnione osoby) i utrzymywana.

UWAGA 2: Zakres dokumentacji SZBI może być odmienny dla różnych organizacji z uwagi na:
- wielkość organizacji i rodzaj działalności;
- zakres i złożoność wymagań bezpieczeństwa oraz zarządzanego systemu.

UWAGA 3: Dokumenty i zapisy mogą przybrać dowolną formę lub być przechowywane na dowolnym typie nośnika.

3.6.1 Zasady tworzenia dokumentacji

Dokumenty wymagane przez SZBI należy chronić i nadzorować. Należy ustanowić udokumentowaną procedurę w celu określenia działań kierownictwa potrzebnych do:

a) zatwierdzenia odpowiednich dokumentów przed ich wydaniem;
b) przeglądu i aktualizacji dokumentów w razie potrzeby oraz ponownego ich zatwierdzania;
c) zapewnienia, że zidentyfikowano zmiany i aktualny status dokumentów;
d) zapewnienia, że najnowsze wersje odpowiednich dokumentów są dostępne w miejscach ich stosowania;
e) zapewnienia, że dokumenty pozostają czytelne i łatwe do zidentyfikowania;
f) zapewnia, że dokumenty są dostępne dla wszystkich, którzy ich potrzebują oraz że są przesyłane, przechowywane i ostatecznie niszczone zgodnie z procedurami odpowiednimi do ich klasyfikacji, w tym także zabezpieczenie przed niepowołanym dostępem;
g) zapewnienia, że dokumenty zewnętrzne są identyfikowane;
h) zapobiegania niezamierzonemu stosowaniu nieaktualnych dokumentów;

3.6.2 Wymagania dotyczące zapisów

W celu dostarczenia świadectwa potwierdzającego zgodność z wymaganiami oraz skutecznej eksploatacji SZBI powinny być ustanowione i utrzymywane odpowiednie zapisy. Zapisy te powinny być chronione i nadzorowane.
SZBI powinien uwzględniać wszystkie odpowiednie wymagania przepisów prawa, wymagania nadzoru i zobowiązania wynikające z umów. Zapisy powinny być czytelne, łatwe do zidentyfikowania i odtwarzalne.
Należy udokumentować i wdrożyć zabezpieczenia służące identyfikowaniu, przechowywaniu, ochronie, odtwarzaniu, archiwizacji oraz niszczeniu zapisów.

Zapisy powinny dotyczyć realizacji procesów mających wpływ na bezpieczeństwo informacji.

PRZYKŁAD
Przykładami zapisów są księgi gości, raporty z audytów wewnętrznych i wypełnione formularze autoryzacji dostępu.

Rozdział IV

Odpowiedzialność kierownictwa

4.1 Zaangażowanie kierownictwa

Kierownictwo firmy badawczej powinno być zaangażowane w ustanowienie, wdrożenie, eksploatację, monitorowanie, przegląd, utrzymanie i doskonalenie SZBI poprzez:

1. Opracowanie, zatwierdzenie i opublikowanie deklaracji bezpieczeństwa informacji, w tym ochrony danych osobowych
2. Zatwierdzenie polityki bezpieczeństwa informacji (zgodnie z pkt. 3.1)
3. Wyznaczenie spośród swego grona oraz formalne powołanie Inspektora Ochrony Danych (IOD) odpowiedzialnego za:

a) ustanowienie polityki bezpieczeństwa informacji;
b) zapewnienie, że cele i plany dotyczące bezpieczeństwa informacji zostały ustanowione;
c) określenie ról i zakresów odpowiedzialności w odniesieniu do bezpieczeństwa informacji;
d) zapewnienie przekazywania pracownikom firmy i stronom trzecim odpowiedniej informacji na temat działań podejmowanych w zakresie bezpieczeństwa informacji, odpowiedzialności prawnej oraz potrzebie ciągłego doskonalenia w tym zakresie;
e) zapewnienie wystarczających zasobów do ustanowienia, wdrażania, eksploatacji monitorowania, przeglądów, utrzymania i doskonalenia SZBI
f) podejmowanie decyzji o kryteriach akceptacji ryzyka i akceptowalnym poziomie ryzyka;
g) zapewnienie przeprowadzania wewnętrznych audytów SZBI;
h) organizowanie i przeprowadzanie przeglądów SZBI.

4.2 Zarządzanie zasobami

4.2.1 Zapewnienie zasobów

Firma badawcza powinna określić i zapewnić zasoby potrzebne do:

a) ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia SZBI;
b) zapewnienia, że procedury bezpieczeństwa informacji wspierają spełnienie wymagań biznesowych;
c) zidentyfikowania i odniesienia się do wymagań przepisów prawa i wymagań nadzoru oraz zobowiązań związanych z bezpieczeństwem, a wynikających z zawartych umów;
d) utrzymania odpowiedniego bezpieczeństwa przez poprawne zastosowanie wszystkich wdrażanych zabezpieczeń;

e) przeprowadzenia przeglądów, kiedy zachodzi taka potrzeba, oraz odpowiedniego reagowania na wyniki tych przeglądów;
f) poprawy skuteczności SZBI tam, gdzie jest to wymagane.

4.2.2 Szkolenie, uświadamianie i kompetencje

Firma badawcza powinna zapewnić, że wszyscy pracownicy etatowi a także koordynatorzy oraz ankieterzy, rekruterzy, audytorzy i inni podwykonawcy wykonujący prace terenowe, z którymi zawarto umowy i którym przypisano zakresy odpowiedzialności określone w SZBI, mają kompetencje do realizacji wymaganych zadań przez:

a) określenie koniecznych kompetencji pracowników i podwykonawców wykonujących prace, które mają wpływ na SZBI;
b) zapewnienie szkolenia lub podjęcie innych działań (np. zatrudnienie specjalistów) w celu realizacji tych potrzeb;
c) ocenę skuteczności zapewnionego szkolenia oraz podjętych działań;
d) prowadzenie zapisów dotyczących edukacji, szkolenia, umiejętności, doświadczenia i kwalifikacji

Firma badawcza powinna zapewnić, aby cały odpowiedni personel był świadomy związku i znaczenia swoich działań dotyczących bezpieczeństwa informacji oraz wkładu dla osiągnięcia celów SZBI.

4.3 Wewnętrzne audyty bezpieczeństwa informacji

Należy zapewnić przeprowadzanie wewnętrznych audytów SZBI w zaplanowanych odstępach czasu, aby określić, czy cele stosowania zabezpieczeń, metody zabezpieczenia, ustalone zasady i procedury są:

a) zgodne z niniejszymi wymaganiami i odpowiednimi ustawami i przepisami;
b) zgodne ze zidentyfikowanym wymaganiami bezpieczeństwa informacji;
c) są skutecznie wdrożone i utrzymywane;
d) zgodne z oczekiwaniami.

Program audytu należy zaplanować, biorąc pod rozwagę status i ważność procesów i obszarów do audytu, jak również wyniki poprzednich audytów. Kryteria audytu, zakres, częstotliwość i metody powinny być zdefiniowane. Wybór audytorów i przeprowadzenie audytu powinny zapewnić obiektywność i bezstronność procesu audytowego. Audytorzy nie powinni audytować swojej własnej pracy.

Wymagania i odpowiedzialność za planowanie i przeprowadzanie audytów oraz za raportowanie wyników i utrzymywanie zapisów powinny być zdefiniowane w udokumentowanej procedurze.

W przypadku gdy w wyniku audytu w obszarze audytowanym zostaną sformułowane uwagi i zalecenia, należy zapewnić aby były one podejmowane i wdrażane bez nadmiernego opóźnienia w celu wyeliminowania wykrytych odstępstw i ich przyczyn.

Po otrzymaniu informacji o wdrożeniu zaleceń z audytu, audytor powinien w ustalonym terminie przeprowadzić weryfikację podjętych w audytowanym obszarze działań i uzyskanych wyników.

4.4 Przeglądy SZBI realizowane przez kierownictwo

Kierownictwo firmy badawczej powinno przeprowadzać przeglądy SZBI w zaplanowanych odstępach czasu (nie rzadziej niż raz w roku) w celu zapewnienia jego ciągłej przydatności, adekwatności i skuteczności. Przegląd powinien zawierać ocenę możliwości doskonalenia i potrzeby zmian, w tym polityki bezpieczeństwa informacji i celów bezpieczeństwa. Wyniki przeglądów powinny być jasno udokumentowane, a odpowiednie zapisy należy przechowywać.

4.4.1 Dane wejściowe do przeglądu

Dane wejściowe do przeglądu realizowanego przez kierownictwo powinny zawierać:

a) wyniki audytów wewnętrznych
b) informacje na temat metod, zasad i procedur, które mogłyby być zastosowane w organizacji, w celu ulepszenia realizacji i skuteczności SZBI;
c) status działań korygujących i zapobiegawczych;
d) podatności lub zagrożenia, do których nie było odpowiedniego odniesienia w poprzednim oszacowaniu ryzyka;
e) działania podjęte na skutek poprzednich przeglądów realizowanych przez kierownictwo;
f) informacje na temat jakiekolwiek zmiany, które mogłyby dotyczyć SZBI;
g) zalecenia dotyczące doskonalenia.

4.4.2 Wyniki przeglądu

Wyniki przeglądu realizowanego przez kierownictwo powinny zawierać informacje dotyczące:

a) szacowania wymaganych zasobów w celu doskonalenia skuteczności SZBI.
b) uaktualnienia planu szacowania ryzyka i postępowania z ryzykiem.
c) udoskonalenia metod pomiaru skuteczności zabezpieczeń.
d) modyfikacji procedur i zabezpieczeń dotyczących bezpieczeństwa informacji, jeśli to konieczne, w celu reakcji na wewnętrzne lub zewnętrzne zdarzenia, które mogą mieć konsekwencje dla SZBI, w tym zmiany:
    1) wymagań biznesowych;
    2) wymagań bezpieczeństwa;
    3) procesów biznesowych mających wpływ na istniejące wymagania bezpieczeństwa;
    4) przepisów prawa i wymagań nadzoru;
    5) zobowiązań wynikających z umów;
    6) poziomów ryzyka i/lub kryteriów akceptacji ryzyka.

4.5 Ciągłe doskonalenie SZBI

Firma badawcza powinna w sposób ciągły poprawiać skuteczność SZBI przez stosowanie polityki bezpieczeństwa informacji, określenie celów bezpieczeństwa informacji, wyników audytu, analizę monitorowanych incydentów, realizację działań korygujących i zapobiegawczych oraz dokonywanie przeglądów realizowanych przez kierownictwo.