WOJSKOWY INSTYTUT MEDYCYNY LOTNICZEJ

Nr ewidencji bibliot. 849/N/2/Zał.1/48

EGZEMPLARZ NADZOROWANY

Polityka Bezpieczeństwa Informacji

Sporządził:		Zatwierdził:	
Pełnomocnik ds. ZSZ	mgr inż. Mirosław Dereń	Dyrektor	płk dr n. med. Alicja TROCHIMIUK
Podpis:		Podpis:	
Data :	7.08.2019	Data :	- 7 LIP. 2019 07.08.2019
Wydanie:	4.1	Wydanie 1.0 wprowadzone zostało Zarządzeniem Dyrektora WIML Nr 9/2011	

Wykonano w 1 Egzemplarzu

Spis treści

Wstęp

Wojskowy Instytut Medycyny Lotniczej w Warszawie jest placówką, której głównym zadaniem jest szeroko pojęta opieka medyczna obejmująca między innymi problematykę oceny stanu zdrowia pilotów samolotów i personelu lotniczego, szeroko pojętą profilaktykę oraz szkolenie w zakresie medycyny lotniczej. Analiza kontekstu WIML, uwzględniającego zmiany organizacyjne w Siłach Zbrojnych RP oraz zmiany w systemie opieki zdrowotnej, wpływa bezpośrednio na wypracowywane decyzje dotyczące organizacji usług świadczonych przez WIML na rzecz lotnictwa i medycyny. Jednocześnie, w ramach Zintegrowanego Systemu Zarządzania (ZSZ) doskonalone są metody zarządzania jakością świadczonych usług i zarządzania bezpieczeństwem informacji.

Szczególną grupę informacji tworzą dane osobowe, których zbiory wykazano w dalszej części dokumentu, a ich ochronę opisano w dokumencie wewnętrznym WIML pn. „Polityka ochrony danych osobowych", zgodnym z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Podstawowe pojęcia

Bezpieczeństwo informacji	-	zachowanie poufności, integralności i dostępności informacji, co oznacza że informacja nie jest ujawniana osobom nieupoważnionym, jest ona dokładna i kompletna oraz jest dostępna w użytecznej formie na żądanie upoważnionego personelu
Zarządzanie ryzykiem i szansą	-	skoordynowane działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka lub szansy
Ryzyko	-	wpływ niepewności na możliwość zrealizowania celu – niedowartościowane ryzyko może pociągnąć za sobą szkodę w organizacji (pośrednio lub bezpośrednio)
Szansa	-	wpływ niepewności podczas określania celu - niedowartościowana szansa może ograniczyć możliwą do uzyskania korzyść. Przewartościowana szansa może skutkować brakiem możliwości uzyskania przewidywanej korzyści ze zrealizowanego celu, bądź wystąpieniem dodatkowych ryzyk.
Ryzyko bezpieczeństwa informacji	-	potencjalnie możliwa sytuacja, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktyw powodując w ten sposób powstanie szkody w komórkach organizacyjnych (w organizacji).
Aktywa	-	wszystko to, co ma wartość dla komórek organizacyjnych (dla Instytutu)
Dane osobowe	-	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.

Wykaz zbiorów danych osobowych

W WIML dane osobowe tworzą następujące zbiory

- Zbiory danych osobowych Ośrodka Klinicznego - dokumentacja papierowa i elektroniczna
- Zbiory części Centrum Medycyny Lotniczej - dokumentacja papierowa
- Zbiory administracyjne - dokumentacja papierowa i elektroniczna

Zbiory finansowe - dokumentacja papierowa i elektroniczna

W grupie danych osobowych zakresem ZSZ objęte są:

- dane osobowe osób badanych i leczonych,
- wyniki badań diagnostycznych,
- treść orzeczeń,
- dane osobowe osób szkolonych.

Opis objętych systemem komórek organizacyjnych WIML

System obejmuje następujące komórki organizacyjne Wojskowego Instytutu Medycyny Lotniczej: Ośrodek Kliniczny, Środowiskową Pracownię Nowych Zastosowań Diagnostycznych Jądrowego Rezonansu Magnetycznego (ŚPNZDJRM), Centrum Medycyny Lotniczej WIML (AeMC WIML), Pion Administracyjny, Pion Ochrony, Zakład Badań Symulatorowych, Szkolenia i Treningu Lotniczo-Lekarskiego (ZBSSiTLL), Zakład Psychologii.

Ośrodek Kliniczny świadczy usługi w zakresie badań lotniczo-lekarskich personelu lotniczego wojskowego, kwalifikacji kandydatów do szkolenia lotniczego i naziemnej obsługi lotów, orzecznictwa w zakresie medycyny pracy diagnozowania i leczenia pacjentów, usługi w zakresie medycznej diagnostyki laboratoryjnej na podstawie zleceń oraz w formie pakietów tworzących profile uwzględniające najczęstsze problemy zdrowotne współczesnego społeczeństwa.
Środowiskowa Pracownia Nowych Zastosowań Diagnostycznych Jądrowego Rezonansu Magnetycznego rozszerza zakres możliwości Ośrodka Klinicznego w obszarze badanń diagnostyki obrazowej.
AeMC WIML świadczy usługi w zakresie badań lotniczo-lekarskich i psychologicznych (ze wskazań) cywilnego personelu lotniczego oraz cywilnego orzecznictwa lotniczego.
ZBSSiTLL świadczy usługi szkolenia w zakresie medycyny lotniczej oraz treningu lotniczego, prowadzonych na bazie naziemnych symulatorów lotniczych, usługi w zakresie udostępniania symulatorów stanowisk badawczych i treningowych obejmujących szkolenie praktyczne w warunkach wysokościowych zmian ciśnienia atmosferycznego, szkolenie praktyczne w zakresie wykonywania manewru przeciwprzeciążeniowego, badań technicznych w warunkach zmiennego przeciążenia, zmiennego ciśnienia i zmiennej temperatury otoczenia.
Zakład Psychologii świadczy usługi na rzecz Ośrodka Klinicznego w zakresie badań lotniczo-lekarskich i psychologicznych personelu lotniczego wojskowego, kwalifikacji kandydatów do szkolenia lotniczego i naziemnej obsługi lotów.
Ośrodek Kliniczny świadczy kompleksowe usługi w zakresie sterylizacji materiałów i narzędzi medycznych.
Pion Administracyjny obsługuje komórki organizacyjne WIML w zakresie kadrowym i logistycznym.

Pion Głównego Księgowego zabezpiecza pozostałe komórki organizacyjne WIML w zakresie obsługi finansowej.
Pion Ochrony zabezpiecza WIML w zakresie ochrony organizacyjnej, technicznej i fizycznej, a także zapewnia sprawną pracę Punktu Ewidencyjnego.
WIML dba o zadowolenie klienta zapewniając wysoki poziom oferowanych usług, świadczonych zgodnie z systematycznie doskonalonymi procedurami. Wprowadzony w Ośrodku Klinicznym, Środowiskowej Pracowni Nowych Zastosowań Diagnostycznych Jądrowego Rezonansu Magnetycznego (ŚPNZDJRM), Centrum Medycyny Lotniczej WIML (AeMC WIML), Pionie Administracyjnym, Pionie Ochrony, Zakładzie Psychologii, Zakładzie Badań Symulatorowych, Szkolenia i Treningu Lotniczo-Lekarskiego (ZBSSiTLL), system zarządzania jakością i bezpieczeństwem informacji jest potwierdzeniem dążenia WIML do osiągnięcia głównego celu, którym jest pełne zadowolenie klienta oraz bezpieczeństwo informacji związanych z klientem i świadczonymi usługami.

Przedmiot działania WIML obejmuje między innymi:

- badania lotniczo-lekarskie i psychologiczne personelu lotniczego,
- orzecznictwo lotniczo-lekarskie,
- orzecznictwo w zakresie medycyny pracy,
- szkolenie w zakresie medycyny lotniczej oraz treningu lotniczego, prowadzonych na bazie naziemnych symulatorów lotniczych,
- uczestniczenie w systemie ochrony zdrowia,
- prowadzenie w sposób ciągły badań naukowych i prac rozwojowych.

Kompletna oferta usług objętych Systemem:

Oferujemy:

1. Wykonywanie badań diagnostycznych :
   - wojskowego i cywilnego personelu lotniczego,
   - pracowników ochrony fizycznej,
   - kierowców i kandydatów na kierowców,
   - ubiegających się lub posiadających pozwolenie na broń
   - ubiegających się o licencję detektywa,
   - osób kierujących działalnością gospodarczą albo bezpośrednio zatrudnionych przy wytwarzaniu i obrocie materiałami wybuchowymi, bronią, amunicją oraz wyrobami o przeznaczeniu wojskowym lub policyjnym,
   - kandydatów do objęcia urzędu sędziego,
   - osób ubiegających się lub posiadających pozwolenie na nabywanie oraz przechowywanie materiałów wybuchowych przeznaczonych do użytku cywilnego (pirotechnicy).
2. Orzecznictwo medyczne w zakresie lotnictwa cywilnego.
3. Orzecznictwo w zakresie medycyny pracy w zakresie podstawowym i odwoławcze.
4. Szkolenie w zakresie medycyny lotniczej.
5. Symulatorowy trening lotniczy w warunkach stacjonarnych i dynamicznych.
6. Badania medyczne w zakresie diagnostyki laboratoryjnej.
7. Sterylizację narzędzi i materiałów.
8. Diagnozowanie i leczenie pacjentów.

Bezpieczeństwo i niezawodność

Bezpieczeństwo zapewnia doświadczony personel wykorzystujący w swojej pracy standardowe, doskonalone przez lata, metody prowadzenia badań i szkolenia oraz nowe rozwiązania w dziedzinie techniki, a także technologii informatycznych.
Osiągnięto wysoki stopień niezawodności usług w oparciu o bieżącą kontrolę stanu wykorzystywanych systemów, wprowadzanie dedykowanych rozwiązań technicznych podnoszących niezawodność systemów oraz bieżącą kontrolę tych systemów. Prowadzi się systematyczną, planową kontrolę organizacji świadczenia usług wspierających procesy badań i szkolenia.

Definicja bezpieczeństwa i zakres systemu

Celem głównym systemu zarządzającego bezpieczeństwem informacji w komórkach organizacyjnych w WIML 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.
Osiągnięcie celu głównego realizowane jest przez cele cząstkowe, które powinny: określać co ma być zrobione, jakie zasoby będą wymagane, kto będzie odpowiedzialny, jaki jest przewidziany termin osiągnięcia celu i jak będą oceniane wyniki.
Cele bezpieczeństwa informacji powinny: być spójne z niniejszą Polityką, być mierzalne (o ile to możliwe), uwzględniać wymagania bezpieczeństwa informacji, analizę i postępowanie z ryzykiem, być aktualizowane (jeśli jest to właściwe).

Deklaracja Dyrektora WIML

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

Dyrektor WIML wprowadzając Politykę Bezpieczeństwa Informacji deklaruje, że wdrożony Zintegrowany System Zarządzania będzie podlegał ciągłemu doskonaleniu, zgodnie z wymaganiami norm ISO 27001, ISO 9001 oraz AQAP 2110. Wdrożony ZSZ, którego składową jest system zarządzający bezpieczeństwem informacji, obejmuje swoim zakresem dane i informacje powierzone przez naszych Klientów oraz informacje własne WIML przetwarzane we wszystkich procesach.

Wyłączono z Deklaracji Stosowania (ISO 27001:2017, pkt. 6.1.3) wymagania niemające zastosowania w WIML, dotyczące: zabezpieczania usług aplikacyjnych w sieciach publicznych - pkt. A.14.1.2 oraz ochrony transakcji usług aplikacyjnych- pkt. A.14.1.3, a także dotyczące prowadzenia prac naukowych i badawczo-rozwojowych - pkt. od A.14.2.1. do A.14.2.6.

Podejście do bezpieczeństwa informacji w WIML 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).

Cele ZSZ w zakresie bezpieczeństwa informacji

Celem wdrożonego systemu zarządzania jakością i bezpieczeństwem informacji jest, między innymi, 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 WIML,
- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa WIML, interesów Instytutu oraz posiadanych i powierzonych Instytutowi 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 WIML,
- 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 WIML zgodnie z wymaganiami normy ISO 27001:2017 i zaleceniami wszystkich zainteresowanych stron.

Zasady ogólne

Każdy pracownik powinien być zapoznany z regułami oraz z kompletnymi i aktualnymi procedurami ochrony informacji w swojej jednostce organizacyjnej. Poniższe uniwersalne zasady są podstawą realizacji polityki bezpieczeństwa informacji:

- **Zasada uprawnionego dostępu**. Każdy pracownik przechodzi szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisuje 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**. WIML świadczy tylko takie usługi jakich wymaga klient.
- **Zasada asekuracji**. Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym (podobnym). W przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie.
- **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych WIML 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 najsłabszego ogniwa**. Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.
- **Zasada kompletności**. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
- **Zasada ewolucji**. Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
- **Zasada odpowiedniości**. Używane mechanizmy muszą być adekwatne do sytuacji.
- **Zasad akceptowanej równowagi**. Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji.
- **Zasada świadomej konwersacji**. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć, co, gdzie i do kogo się mówi.

-

Organizacja bezpieczeństwa informacji

Struktura zarządzania bezpieczeństwem

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 audytu bezpieczeństwa przy zapewnieniu rękojmi zachowania tajemnicy

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

Koncepcja dokumentacji systemu zarządzania bezpieczeństwem informacji

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

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

Struktura zarządzania bezpieczeństwem i podział odpowiedzialności

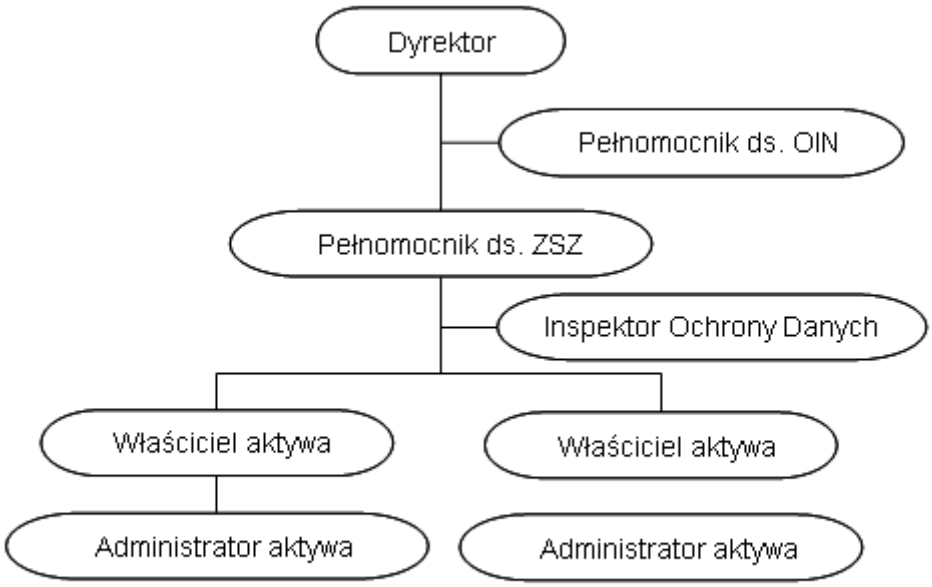
Odpowiedzialność za bezpieczeństwo informacji w WIML ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków.

- Dyrektor WIML odpowiedzialni są za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz poszczególnych zabezpieczeń. Dyrektor wydaje zgodę na użytkowanie urządzeń służących do przetwarzania informacji i zabezpieczeń rekomendowanych przez Pełnomocnika ds. Ochrony Informacji Niejawnych (OIN), Inspektora Ochrony Danych (IOD), w porozumieniu z kierownikiem Pracowni Informatyki.
- Dyrektor WIML decyduje również o współpracy w zakresie bezpieczeństwa z innymi podmiotami. Dyrektor może również wyrazić zgodę na udostępnienie stronom trzecim informacji stanowiących tajemnicę WIML. Codzienne postępowanie Dyrektora WIML stanowi przykład dla innych pracowników,

że aspekty bezpieczeństwa informacji posiadają wysoki priorytet we wszystkich podejmowanych i planowanych działaniach.

- Pełnomocnik ds. Zintegrowanego Systemu Zarządzania odpowiedzialny jest za koordynację działań zapewniających bezpieczeństwo informacji oraz związanych z nim polityk i procedur w obszarze objętym systemem.
- Właściciel aktywa odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem
- Administrator aktywa odpowiada za realizację i nadzór nad technicznymi aspektami aktywa w ścisłej kooperacji z Właścicielem aktywa.

Poniższy schemat (Rys. 1) przedstawia organizację zarządzania bezpieczeństwem informacji w WIML, w obszarze objętym systemem.



Rys. 1 Organizacja zarządzania bezpieczeństwem informacji w WIML

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 zaangażowany jest dyrektor WIML określający zasadnicze użytkowe kryteria bezpieczeństwa informacji (pochodne od kryteriów 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).

Zasady współpracy z osobami trzecimi

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

- do podpisania umowy lojalnościowej o przestrzeganiu tajemnicy służbowej i ochronie danych osobowych,
- 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 nie zostaje pozostawiona bez nadzoru personelu WIML. Dostęp do magazynów i biur wszelkiego personelu technicznego zajmującego się konserwacją sprzętu, ochrony, partnerów handlowych i innych osób jest nadzorowany przez pracowników WIML.

Dostęp gości w oznaczonych strefach bezpieczeństwa jest ograniczony.

Zasady współpracy z innymi podmiotami

Współpraca WIML z innymi podmiotami oparta jest na umowach, regulaminach lub zarządzeniach. WIML ma zawsze na względzie, aby obejmowały one deklarację o zachowanie poufności oraz zobowiązania do działania zgodnie z prawem.

Zasady współpracy z Policją, Żandarmerią Wojskową, Strażą Pożarną i Strażą Miejską

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, lub Żandarmeria Wojskowa,
- 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 i Żandarmerii Wojskowej.
- Niezwłocznego przekazania Policji lub Żandarmerii Wojskowej osób stwarzających, w sposób oczywisty, zagrożenie dla życia lub zdrowia ludzkiego, a także chronionego obiektu.

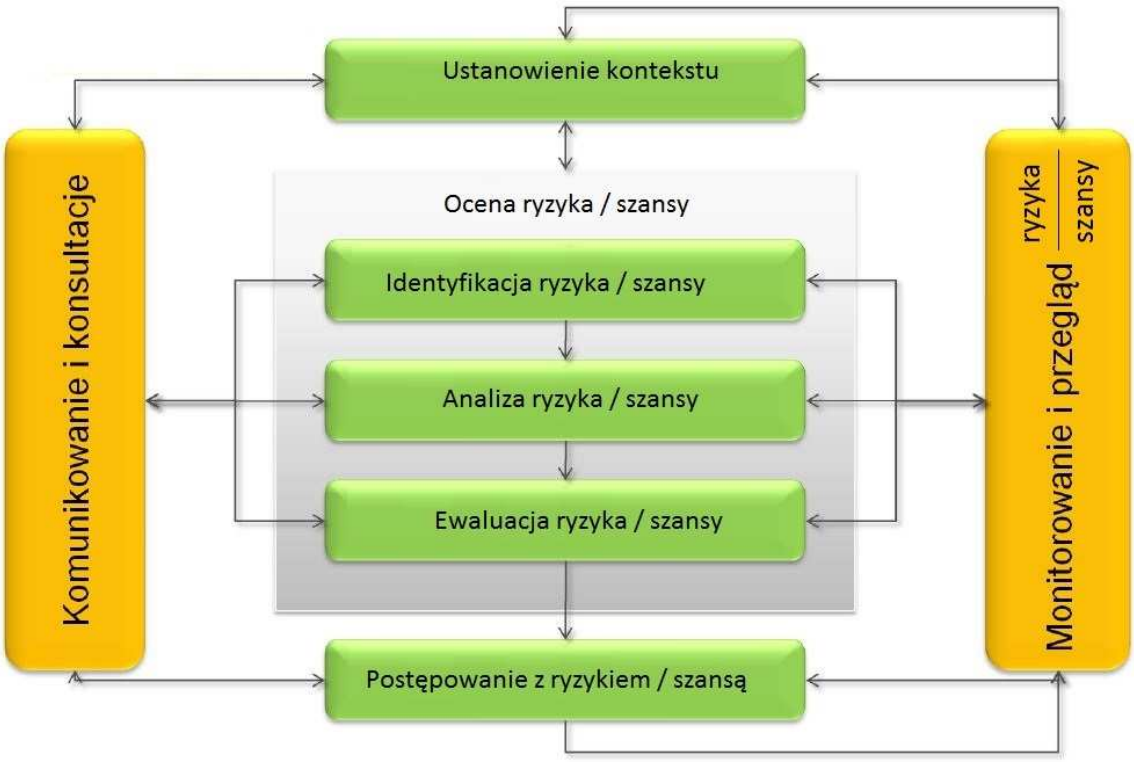
Zabezpieczenie mienia WIML na wypadek pożaru lub awarii:

- o zaistniałym pożarze lub awarii pracownik natychmiast zawiadamia:
  - osoby znajdujące się w strefie zagrożenia,
  - Straż Pożarną,
  - służby dyżurne WIML,
  - do czasu przybycia jednostek ratowniczych, lub osób funkcyjnych podejmuje działania mające na celu:
    - ugaszenie ognia,
    - udzielenie pomocy osobom poszkodowanym lub zagrożonym,
    - zabezpieczenie, w miarę możliwości, mienia oraz dokumentacji przed pożarem i osobami postronnymi.
- Przybyłe jednostki ratownicze natychmiast kieruje na miejsce akcji.

Informacje kontaktowe dostępne są na dyżurce WIML.

Zarządzanie aktywami i ryzykiem

WIML uważnie zarządza swoimi aktywami informacyjnymi. Celem takiego postępowania jest zapewnienie im wymaganego poziomu bezpieczeństwa i właściwego zidentyfikowania i wykorzystania szans.



Rys.2 Schemat procesu zarządzania ryzykiem lub szansą

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

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

Podstawowym **kryterium akceptacji ryzyk** jest dążenie do wyrównania ich poziomów. 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.

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 dokumentach, za dopuszczenie do użytkowania nowych urządzeń odpowiada Dyrektor WIML.

Bezpieczeństwo zasobów ludzkich

WIML 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. Pracownicy są okresowo oceniani pod względem spełnienia wymagań bezpieczeństwa oraz szkoleni z tej tematyki.

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

Bezpieczeństwo fizyczne i środowiskowe

WIML 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 siedzibie WIML w odniesieniu do informacji. W przypadku danych od naszych Klientów najistotniejsze jest zapewnienie wszystkich trzech podstawowych aspektów bezpieczeństwa poufności danych oraz ich 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.

Kluczowe systemy techniczne i informatyczne wyposażone są w systemy podtrzymujące zasilanie.

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

Zarządzanie systemami i sieciami

WIML 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 WIML.
- opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy.
- kontrolowaniu wprowadzania wszelkie zmian do infrastruktury technicznej.
- w celu zapewnienia bezpieczeństwa podstawowych systemów usługowych, 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.
- WIML monitoruje poziom incydentów w systemach informatycznych i posiada mechanizmy reagowania w przypadkach ich wystąpienia.

Kontrola dostępu

WIML 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. Pomieszczenia biurowe w firmie zamykane są na klucz, a pomieszczenia szczególnie istotne chronione są elektronicznymi systemami kontroli i dostępu. Obiekt poza jest ciągle monitorowany przez służbę ochrony.

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

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.

Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych

WIML zapewnia, ze wszystkie procesy związane z pozyskaniem, rozwojem bądź utrzymaniem systemów informacyjnych, w tym systemów i aplikacji informatycznych własnych i/lub Partnerów, wykorzystywanych wewnętrznie lub oferowanych Klientom, prowadzone jest 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

Zarządzanie incydentami

W przypadku wystąpienia incydentów w WIML powiadamiany jest Pełnomocnik ds. Zintegrowanego Systemu Zarządzania. 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 zapisywane w rejestrze zbiorczym, a następnie analizowane są przez Pełnomocnika ds. ZSZ i w razie potrzeby przez właściwe osoby funkcyjne.

Zarządzanie ciągłością działania

WIML 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. Powyższe zasady zapewniają, że WIML jest przygotowany na działanie również w przypadkach odbiegających od normy.

Zgodność

WIML 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 innych 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 techniczną stosowanych urządzeń oraz prowadzone są audyty wewnętrzne funkcjonowania systemu.

Postanowienia końcowe

WIML 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 Pełnomocnik ds. ZSZ, będący reprezentantem Dyrektora WIML.

Naruszenia świadome, bądź przypadkowe niniejszej Polityki Bezpieczeństwa Informacji (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 właściwy dla miejsca sprawy.

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

- Firmami certyfikującymi na zgodność ze standardami bezpieczeństwa i jakością świadczonych usług, w tym na zgodność z normą ISO 27001, ISO 9001 i AQAP 2110
- Ekspertami w zakresie bezpieczeństwa
- oraz pozostałymi instytucjami (Klientami, Dostawcami, Partnerami i innymi zainteresowanymi stronami).

Wykaz zmian

Lp.	Data zmiany	Nr strony	Krótki opis zmiany *(num. stron wg. wyd. 4.1)*	Wprowadził
Zmiany w wydaniu 4.0				
1	7.08.2019	3	We wstępie odniesiono się do analizy kontekstu	M. Dereń
2	7.08.2019	4	Usunięto nieaktualny zapis ustawy	M. Dereń
3	7.08.2019	4, 5	Dodano w opisie Środowiskową Pracownię Nowych Zastosowań Diagnostycznych Jądrowego Rezonansu Magnetycznego	M. Dereń
4	7.08.2019	6	Uproszczono zapis wymagań niemających zastosowania	M. Dereń
	7.08.2019	9	Dostosowano do wymagań normy zakres odpowiedzialności	M. Dereń
5	7.08.2019	10	Uaktualniono schemat zarządzania (Rys.1)	M. Dereń
	7.08.2019	13	Ujednolicono zasady dopuszczania urządzeń do przetwarzania informacji	M. Dereń
	7.08.2019	15	Urealniono sposób analizy zgłoszonych incydentów	M. Dereń
Zmiany w wydaniu 4.1				
1	17.10.2019	2, 7	Wyodrębniono osobny podrozdział pt. „Cele ZSZ w zakresie bezpieczeństwa informacji”	M. Dereń
2				
3				
4				
5				
6				
7				
8				