Elementy wymagań ISO/IEC 27001 i zalecenia ISO/IEC 17799 osobowe

dr inż. Bolesław Szomański

bolkosz@wsisiz.edu.pl

Filozofia prezentacji wymagań i zabezpieczeń zgodnie z załącznikiem A

- **Nagłówek rozdziały normy ISO 17799**
- Obszary tematyczne - o różnym poziomie komplikacji
- ***Cele zabezpieczenia (objectives*)**
- **Wymagania dotyczące stosowania zabezpieczeń (z ISO 27001)**
- **Zalecenia z ISO/IEC 17799 (27002)**
- **Wskazówki realizacji (*implementation guidance*)**

8 - Bezpieczeństwo zasobów ludzkich

- **A 8.1 Przed zatrudnieniem**
- **A 8.2 Podczas zatrudnienia**
- **A 8.3 Zakończenie lub zmiana zatrudnienia**

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem **(1)**

- ***A.8.1.** Cel zabezpieczania:*
  - *Zapewnienie, że*
    - *pracownicy,*
    - *wykonawcy oraz*
    - *użytkownicy reprezentujący stronę trzecią*
  - *rozumieją swoje obowiązki,*
    - *są odpowiedni do pełnienia obowiązków,*
      - ***które mają być im powierzone, oraz***
  - *Zredukowanie*
    - *ryzyka kradzieży,*
    - *naruszenia i*
    - *niewłaściwego korzystania z urządzeń.*

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (2)

- *A.8.1.1. Role i odpowiedzialności*
  - **Role i odpowiedzialności**
    - pracowników,
    - wykonawców oraz
    - użytkowników reprezentujących stronę trzecią z
  - o **zakresu bezpieczeństwa**
  - o **powinny zostać określone i**
  - o **udokumentowane**
    - zgodnie z polityką bezpieczeństwa informacji organizacji.

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (1)

- **Zaleca się, aby**
  - **zakres obowiązków zawierał**
    - o **wymagania odnoszące się do:**
  - **działań zgodnych z**
    - o **politykami bezpieczeństwa informacji organizacji (patrz 5.1);**
  - **ochrony aktywów przed**
    - o **nieuprawnionym dostępem,**
    - o **ujawnieniem,**
    - o **modyfikacją,**
    - o **zniszczeniem lub**
    - o **zniekształceniem;**

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (3)

- **wykonywania konkretnych działań i procesów bezpieczeństwa;**
- **określenia odpowiedzialności osoby za jej działania;**
- **raportowania zdarzeń związanych lub**
  - o **potencjalnie związanych z bezpieczeństwem oraz**
  - o **innych ryzyk bezpieczeństwa.**

- **Zaleca się, aby role i odpowiedzialności**
  - **w zakresie bezpieczeństwa były**
    - o **określone i**
    - o **w jasny sposób przekazane**
    - o **kandydatom podczas procesu rekrutacji.**

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (4)

- *A.8.1.2 Postępowanie sprawdzające*
  - **Powinno się przeprowadzić weryfikację**
    - wszystkich kandydatów do zatrudnienia,
    - wykonawców oraz
    - użytkowników reprezentujących stronę trzecią
  - o **zgodnie z mającymi zastosowanie**
  - o **przepisami prawa,**
  - o **regulacjami wewnętrznymi i**
  - o **etyką**
    - oraz
  - o **proporcjonalnie do**
    - wymagań biznesowych,
    - klasyfikacji informacji,
      - *która ma być udostępniona, oraz*
    - dostrzeżonych ryzyk.

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (4)

- **Postępowanie sprawdzające:**
  - **wymaganie przedstawienia**
  - **satysfakcjonujących referencji, np.**
    - **jednego świadectwo pracy i**
    - **jednej referencji osobistej;**
  - **sprawdzenie**
    - **(kompletności i dokładności)**
    - **przedstawionego życiorysu;**
  - **potwierdzenie deklarowanego**
    - **wykształcenia i**
    - **kwalifikacji zawodowych;**
  - **niezależne potwierdzenie tożsamości**
    - **(paszport lub podobny dokument);**
  - **bardziej szczegółowe sprawdzenia,**
    - takie jak
    - **sprawdzenie zadłużenia lub**
    - **niekaralności.**

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (5)

- **Jeśli stanowisko,**
  - **wymaga przyznania dostępu do**
  - **środków służących do przetwarzania informacji wrażliwych**
  - **to zaleca się, aby**
    - **rozważono w organizacji**
  - **przeprowadzenie dalszego,**
  - **bardziej szczegółowego sprawdzenia.**
- **Zaleca się, aby**
  - **procedury definiowały kryteria i**
    - **ograniczenia postępowania sprawdzającego,**
      - np. kto odpowiada za przeprowadzenie postępowania,
      - jak, kiedy i dlaczego
      - postępowanie sprawdzające jest przeprowadzane

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (6)

- **Zaleca się przeprowadzenie postępowania sprawdzającego**
  - **także wobec wykonawców oraz**
  - **użytkowników reprezentujących stronę trzecią.**
- **Jeśli wykonawcy są rekrutowani za pośrednictwem agencji,**
  - **to zaleca się, umieszczenie odpowiedzialności w umowie**
- **Zaleca się, aby**
  - **umowy ze stronami trzecimi (patrz 6.2.3)**
  - **jasno określały wszystkie odpowiedzialności oraz**
  - **procedury powiadamiania związane z postępowaniem sprawdzającym.**
- **Zaleca się, aby**
  - **informacje o kandydatach były**
  - **przechowywane i**
  - **przetwarzane zgodnie z odpowiednimi przepisami prawa.**
- **Zaleca się, aby kandydaci byli uprzedzeni o przeprowadzaniu postępowania sprawdzającego.**

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (7)

- ***A.8.1.3. Zasady i Warunki zatrudnienia***
  - **Uzgodnienie i**
  - **podpisanie**
    - **zasad i**
    - **warunków umowy zatrudnienia**
    - **Powinno być**
  - **częścią zobowiązań kontraktowych**
    - pracowników,
    - wykonawców oraz
    - użytkowników reprezentujących stronę trzecią
  - **precyzującej ich obowiązki oraz**
  - **obowiązki organizacji**
    - w zakresie bezpieczeństwa.

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (8)

- **Zaleca się aby**
  - **pracownicy,**
  - **wykonawcy oraz**
  - **użytkownicy reprezentujący stronę trzecią, którym**
    - przyznaje się dostęp do informacji wrażliwych,
  - **podpisali umowę o poufności i nie ujawnianiu informacji**
  - **przed uzyskaniem dostępu do środków służących do przetwarzania informacji;**
- **prawa i obowiązki**
  - **pracowników,**
  - **wykonawców oraz**
  - **innych użytkowników,**
    - np. w odniesieniu do **praw autorskich** lub **ochrony danych osobowych** (patrz 15.1.1 i 15.1.2);

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (8)

- **obejmowały**
- **obowiązek**
  - **klasyfikacji informacji i**
  - **zarządzania aktywami organizacji**
    - związanymi z systemami **informacyjnymi** i
    - **usługami** obsługiwanymi przez
      - **pracownika**,
      - **wykonawcę** *oraz*
      - **użytkownika** *reprezentującego stronę* **trzecią** *(patrz 7.2.1 i 10.7.3);*
- **obowiązki**
  - pracowników,
  - wykonawców oraz
  - użytkowników reprezentujących stronę trzecią
  - **w zakresie przetwarzania informacji**
    - otrzymywanej z **innych firm** lub
    - stron **zewnętrznych**;

8 - Bezpieczeństwo zasobów ludzkich

8.1 – Przed zatrudnieniem (9)

- **obowiązki organizacji**
  - **w zakresie przetwarzania danych osobowych pracownika,**
    - w tym informacji tworzonych w wyniku lub
    - w trakcie zatrudnienia w organizacji (patrz 15.1.4);
- **obowiązki, które są**
  - **rozszerzone poza siedzibę organizacji oraz**
  - **poza normalne godziny pracy,**
    - np. w przypadku wykonywania pracy w domu (patrz 9.2.5 i 11.7.1);
- **działania podejmowane,**
  - jeśli pracownik,
  - wykonawca lub
  - użytkownik reprezentującego stronę trzecią
  - **nie przestrzega wymagań bezpieczeństwa organizacji (patrz 8.2.3).**

8 - Bezpieczeństwo zasobów ludzkich 8.1 – Przed zatrudnieniem (10)

- **Zaleca się, aby organizacja zapewniła, że**
  - **pracownicy,**
  - **wykonawcy oraz**
  - **użytkownicy reprezentujący stronę trzecią**
  - **akceptują zasady i warunki**
    - **związane z bezpieczeństwem informacji,**
    - **odpowiednie do rodzaju i zakresu**
    - **przyznanego im dostępu do aktywów organizacji powiązanych z systemami informacyjnymi i usługami.**
- **Zaleca się,**
  - **aby w uzasadnionych przypadkach,**
  - **obowiązki zawarte w zasadach i warunkach zatrudnienia**
    - **rozciągały się na określony czas**
  - **po ustaniu stosunku pracy (patrz 8.3).**

8 - Bezpieczeństwo zasobów ludzkich

8.2 – Podczas zatrudnienia (1)

- **A.8.2. Podczas zatrudnienia**
  - **Cel: *Zapewnienie, że***
    - *pracownicy,*
    - *wykonawcy oraz*
    - *użytkownicy reprezentujący stronę trzecią są*
    - ***świadomi zagrożeń i***
      - *innych aspektów bezpieczeństwa informacji,*
        - swoich obowiązków i
        - odpowiedzialności prawnej oraz
    - ***są wyposażeni w środki do***
    - ***wspomagające politykę bezpieczeństwa organizacji***
    - ***podczas swej normalnej pracy,***
      - a minimalizujące
    - ***ryzyko błędów ludzkich.***

8 - Bezpieczeństwo zasobów ludzkich

8.2 – Podczas zatrudnienia (2)

- **A.8.2.1 Obowiązki kierownictwa**
  - **Kierownictwo powinno**
    - **wymagać od**
      - pracowników,
      - wykonawców oraz
      - użytkowników reprezentujących stronę trzecią
    - **stosowania bezpieczeństwa**
    - **zgodnie z wprowadzonymi w organizacji**
    - **politykami i**
    - **procedurami.**

8 - Bezpieczeństwo zasobów ludzkich

8.2 – Podczas zatrudnienia (2)

- **Zaleca się, aby kierownictwo było**
  - **zobowiązane do zapewnienia, że**
    - pracownicy,
    - wykonawcy oraz
    - użytkownicy reprezentujący stronę trzecią:
  - **są informowani o swoich obowiązkach**
    - **związanych z bezpieczeństwem informacji**
    - **przed przyznaniem im dostępu do**
    - **wrażliwych informacji lub systemów informacyjnych;**
  - **otrzymują zalecenia**
    - **określające wymagania w**
    - **zakresie bezpieczeństwa związane z ich**
      - obowiązkami w organizacji;

8 - Bezpieczeństwo zasobów ludzkich

8.2 – Podczas zatrudnienia (3)

- **są motywowani do stosowania**
  - **polityk bezpieczeństwa organizacji;**
- **osiągają poziom świadomości bezpieczeństwa**
  - **odpowiedni do swoich obowiązków w organizacji (patrz 8.2.2);**
- **wypełniają zalecenia i warunki zatrudnienia, które**
  - **uwzględniają politykę bezpieczeństwa informacji organizacji oraz**
  - **właściwe metody pracy;**
- **w sposób ciągły utrzymują**
  - **odpowiednie umiejętności i kwalifikacje.**

8 - Bezpieczeństwo zasobów ludzkich

8.2 – Podczas zatrudnienia (4)

- *A8.2.2* ***Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji***
  - Wszyscy
    - **pracownicy organizacji**
      - ***oraz, gdzie jest to wskazane,***
    - **wykonawcy i**
    - **użytkownicy reprezentujący stronę trzecią**
  - powinni zostać odpowiednio przeszkoleni oraz
  - być regularnie informowani o
    - uaktualnieniach
  - polityk i procedur
    - obowiązujących w organizacji,
      - **które są związane z wykonywaną**
    - przez nich pracą.

8 - Bezpieczeństwo zasobów ludzkich

8.2 – Podczas zatrudnienia (5)

- **Zalecenia**
  - **szkolenia uświadamiające**
    - **przeprowadzać przed przyznaniem**
    - **dostępu do informacji lub usług i**
    - **rozpoczynać je od formalnego wprowadzenia polityki oraz wymagań bezpieczeństwa organizacji.**
  - **Aby szkolenie obejmowało**
    - **wymagania bezpieczeństwa,**
    - **zabezpieczenia wynikające z zobowiązań prawnych i biznesowych oraz**
    - **dotyczyło właściwego korzystania z środków służących do przetwarzania informacji,**
      - np. procedur logowania, korzystania z pakietów oprogramowania oraz
    - **postępowanie dyscyplinarne (patrz 8.2.3).**

8 - Bezpieczeństwo zasobów ludzkich

8.2 – Podczas zatrudnienia (6)

- **A.8.2.3. Postępowanie dyscyplinarne**
  - **Wobec pracowników,**
    - **którzy naruszyli**
    - **procedury i polityki bezpieczeństwa organizacji**
  - **powinien być wdrożony**
    - **formalny proces postępowania dyscyplinarnego**

8 - Bezpieczeństwo zasobów ludzkich

8.2 – Podczas zatrudnienia (6)

- **Zalecenia**
  - **Postępowania dyscyplinarnego**
    - **nie należy rozpoczynać**
    - **bez uprzedniej weryfikacji,**
  - **że nastąpiło**
  - **naruszenie bezpieczeństwa**
    - **(patrz 13.2.3 – gromadzenie materiału dowodowego).**

8 - Bezpieczeństwo zasobów ludzkich

8.2 – Podczas zatrudnienia (7)

- Zaleca się, aby formalne postępowanie dyscyplinarne zapewniało
  - poprawne i obiektywne traktowanie pracowników, którzy podejrzani są o naruszenie bezpieczeństwa.
- Zaleca się, aby to postępowanie było
  - stopniowane, uwzględniało takie czynniki,
  - jak natura i ciężar naruszenia, jego wpływ na biznes, czy jest to
  - pierwsze, czy kolejne naruszenie, czy winny został prawidłowo przeszkolony, właściwe przepisy prawne lub inne stosowne czynniki.
- W poważnych przypadkach naruszeń, zaleca się, aby postępowanie dopuszczało
  - natychmiastowe zwolnienie z obowiązków, odebranie praw dostępu i przywilejów oraz, jeśli to konieczne,
  - natychmiastowe wydalenie pod strażą z siedziby organizacji..

8 - Bezpieczeństwo zasobów ludzkich

8.3 – Zakończenie lub zmiana zatrudnienia (1)

- A.8.3. Zakończenie lub zmiana zatrudnienia
  - *Cel: Zapewnienie, że*
    - *pracownicy,*
    - *wykonawcy i*
    - *użytkownicy reprezentujący stronę trzecią*
    - o *odchodzą z organizacji lub*
    - o *zmieniają stanowisko w sposób zorganizowany.*
- A 8.3.1 Odpowiedzialności związane z zakończeniem zatrudnienia
  - Odpowiedzialności związane z
    - o zakończeniem lub
    - o zmianą zatrudnienia powinny być
    - o jasno określone i przypisane.

8 - Bezpieczeństwo zasobów ludzkich

8.3 – Zakończenie lub zmiana zatrudnienia (2)

- Zaleca się, aby przekazywanie odpowiedzialności przy zakończeniu zatrudnienia odnosiło się do
  - Istniejących wymagań bezpieczeństwa,
  - zobowiązań prawnych oraz tam, gdzie to stosowne,
  - odpowiedzialności wynikającej z umowy o zachowaniu poufności (patrz 6.1.5) oraz
  - zasad i warunków zatrudnienia (patrz 8.1.3), które
  - trwają przez określony czas po ustaniu stosunku pracy
    - o pracownika,
    - o wykonawcy lub
    - o użytkownika reprezentującego stronę trzecią.

8 - Bezpieczeństwo zasobów ludzkich

8.3 – Zakończenie lub zmiana zatrudnienia (3)

- Zaleca się, aby te obowiązki i odpowiedzialności, które pozostają w mocy po ustaniu stosunku pracy
  - zawierać w umowach pracowników, wykonawców i użytkowników reprezentujących stronę trzecią.
- Zaleca się, aby zmiany obowiązków lub zatrudnienia były traktowane jak
  - zakończenie wykonywania odpowiednich obowiązków lub zatrudnienia, a
  - przyjęcie nowych obowiązków lub zatrudnienie było przeprowadzone zgodnie z rozdziałem 8.1

8 - Bezpieczeństwo zasobów ludzkich

8.3 – Zakończenie lub zmiana zatrudnienia (4)

- **A.8.3.2 Zwrot aktywów**
  - **Wszyscy**
    - pracownicy,
    - wykonawcy i
    - użytkownicy reprezentujący stronę trzecią
  - **powinni zwrócić wszystkie posiadane aktywa organizacji**
  - **przy zakończeniu stosunku pracy,**
    - kontraktu lub
    - umowy.

8 - Bezpieczeństwo zasobów ludzkich

8.3 – Zakończenie lub zmiana zatrudnienia (4)

- **Zaleca się, aby sformalizować proces zakończenia zatrudnienia tak, aby**
  - **obejmował zwrot wydanego oprogramowania,**
  - **dokumentów i sprzętu,**
  - **jak również innych aktywów organizacji, takich jak**
    - **przenośne urządzenia do przetwarzania danych,**
    - **karty kredytowe,**
    - **karty dostępowe,**
    - **oprogramowanie,**
    - **podręczniki oraz**
    - **informacje przechowywane na mediach elektronicznych.**

8 - Bezpieczeństwo zasobów ludzkich

8.3 – Zakończenie lub zmiana zatrudnienia (5)

- **W przypadkach gdy pracownicy, wykonawcy i użytkownicy reprezentujący stronę trzecią**
  - **wykupują sprzęt organizacji lub korzystają z własnego,**
  - **zaleca się postępowanie zgodne z procedurami zapewniającymi, że wszystkie odpowiednie**
  - **informacje zostaną przekazane organizacji i**
  - **w bezpieczny sposób usunięte ze sprzętu (patrz 10.7.1).**
- **W przypadku, gdy pracownicy, wykonawcy i użytkownicy reprezentujący stronę trzecią**
  - **dysponują wiedzą na temat toczących się operacji,**
  - **zaleca się jej udokumentowanie i przekazanie organizacji.**

8 - Bezpieczeństwo zasobów ludzkich

8.3 – Zakończenie lub zmiana zatrudnienia (6)

- **8.3.3 Odebranie praw dostępu**
  - **Prawa dostępu**
    - pracowników,
    - wykonawców i
    - użytkowników reprezentujących stronę trzecią
  - **do informacji lub**
  - **środków służących do jej przetwarzania.**
  - **Powinny być odebrane**
  - **zakończenia albo**
  - **zmiany zatrudnienia,**
    - kontraktu lub
    - umowy
      - *lub*
    - zmodyfikowane zgodnie
    - z zaistniałymi zmianami zatrudnienia

8 - Bezpieczeństwo zasobów ludzkich

8.3 – Zakończenie lub zmiana zatrudnienia (7)

- Przy zakończeniu zatrudnienia zaleca się przegląd praw dostępu do aktywów związanych z systemami informacyjnymi i usługami.
  - W ten sposób można zdecydować, czy zachodzi potrzeba odebrania praw dostępu.
- Zaleca się, aby zmiany w zatrudnieniu były odzwierciedlone
  - w odebraniu wszystkich praw, które są nieuzasadnione w związku z nowymi obowiązkami.
- Prawa dostępu, które zaleca się odebrać lub dostosować,
  - obejmują
    - dostęp fizyczny i logiczny,
    - klucze,
    - karty identyfikacyjne,
    - środki służące do przetwarzania informacji (patrz 11.2.4),
    - subskrypcje