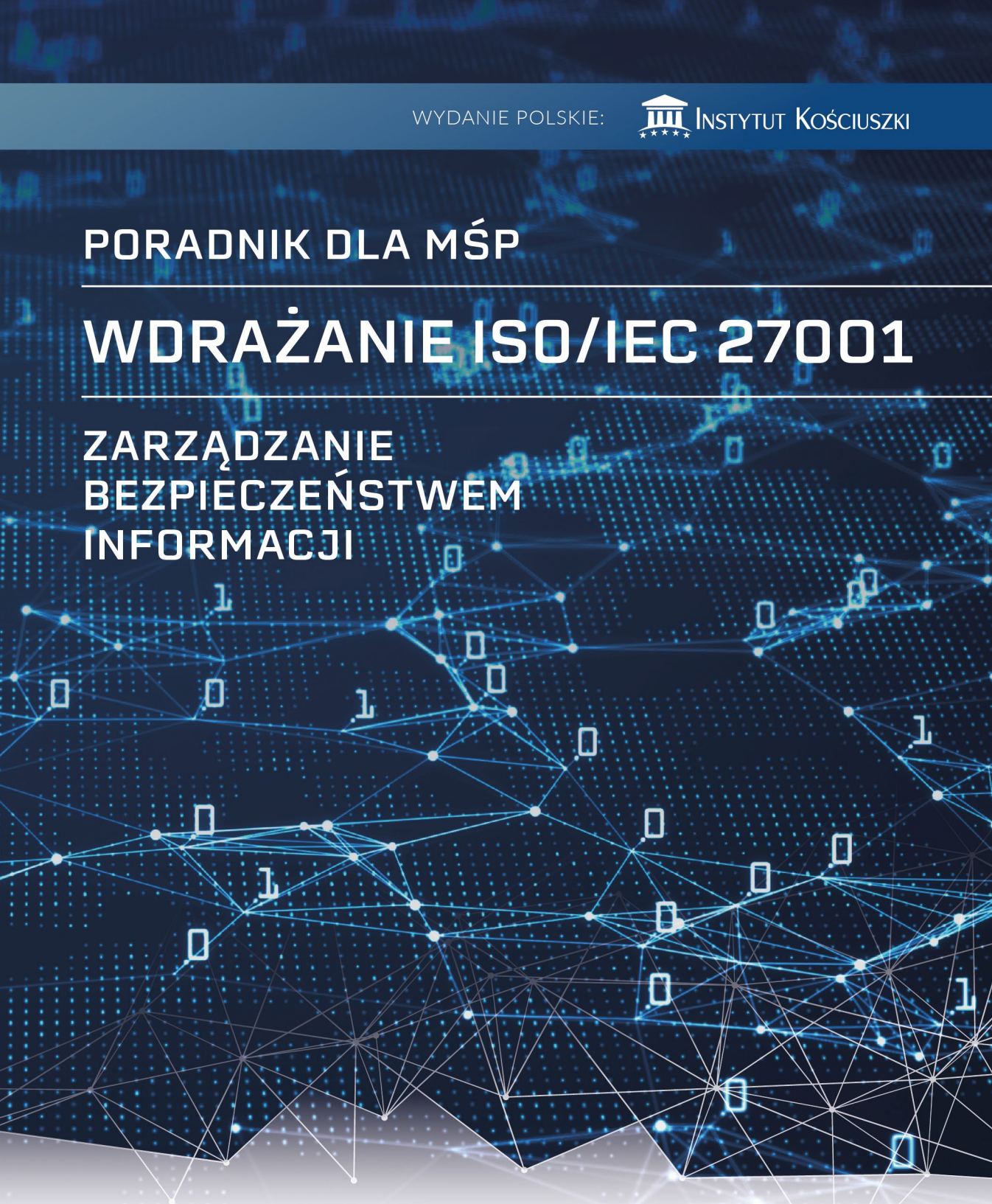
WYDANIE POLSKIE: INSTYTUT KOŚCIUSZKI

PORADNIK DLA MŚP

WDRAŻANIE ISO/IEC 27001

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI



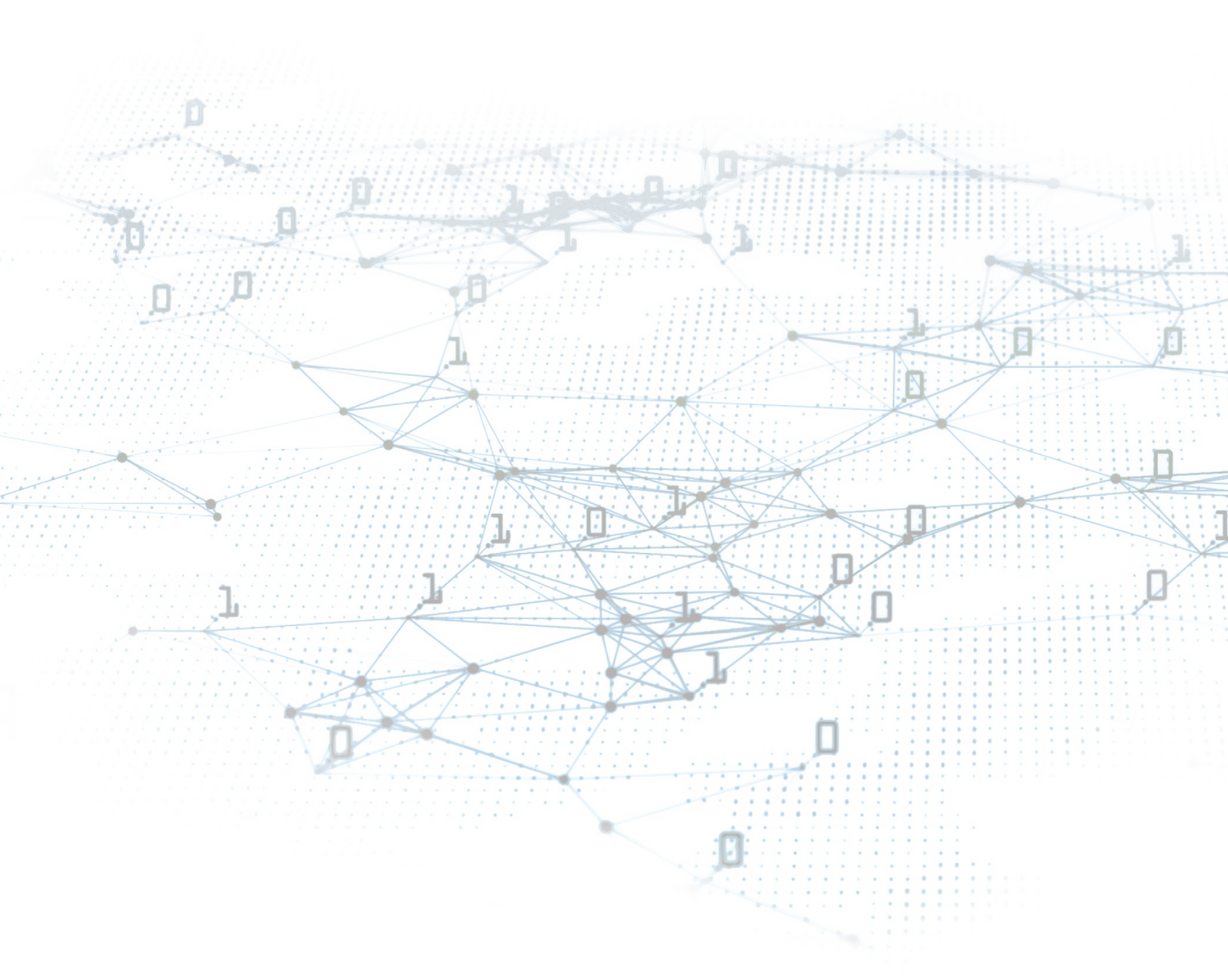
Small Business Standards

European DIGITAL SME Alliance

EFTA

European Commission

Publikacja współfinansowany przez Komisję Europejską oraz Europejskie Stowarzyszenie Wolnego Handlu (EFTA)



PORADNIK DLA MŚP

WDRAŻANIE ISO/IEC 27001

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

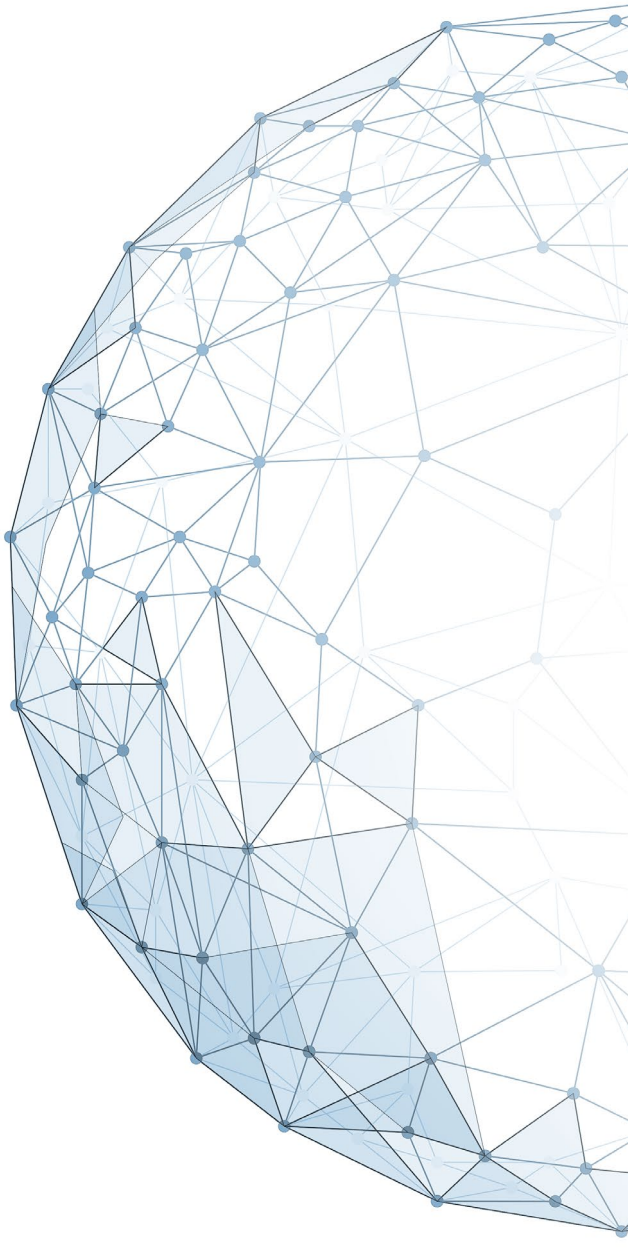
PREZES:
Fabio Guasconi

KOORDYNATOR:
Guido Sabatini

ZESPÓŁ EKSPERTÓW:
Georgia Papadopoulou
George I. Sharkov
David Bulavrishvili
Sergio Oteiza
Holger Berens
Sebastiano Toffaletti
Nanuli Chkhaidze
Yuri V. Metchev
Thorsten Dombach
Alexander Häußler

REDAKTORZY WYDANIA POLSKIEGO:
Agnieszka Górniak
Robert Siudak
Barbara Sztokfisz

TŁUMACZENIE:
Instytut Kościuszki



Publikacja została przygotowana w ramach projektu „Standaryzacja usług Hubów Innowacji Cyfrowej dla wsparcia cyfrowej transformacji przedsiębiorstw" współfinansowanego z Programu Ministra na lata 2019-2021 p.n. „Przemysł 4.0."

PRZEDMOWA

Europejskie Stowarzyszenie Małych i Średnich Przedsiębiorstw Cyfrowych (ang. European DIGITAL SME Alliance) jest największą siecią małych i średnich przedsiębiorstw (MŚP) sektora ICT w Europie, reprezentującym około 20 tys. cyfrowych MŚP. To wspólna inicjatywa 28 krajowych i regionalnych stowarzyszeń MŚP z krajów członkowskich UE oraz państw sąsiadujących, dążąca do umieszczenia cyfrowych MŚP w centrum agendy UE.

DIGITAL SME jest członkiem Small Business Standards (SBS), europejskiej organizacji reprezentującej MŚP w procesie standaryzacji, zgodnie z Aneksem III do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012. Chcąc przyspieszyć wdrażanie Programu Działań SBS na rok 2017 współfinansowanego przez Komisję Europejską oraz Europejskie Stowarzyszenie Wolnego Handlu, DIGITAL SME opracowało niniejszy poradnik dla MŚP na temat wdrażania systemu bezpieczeństwa informacji zgodnego z normą ISO/IEC 27001.

Niniejszy poradnik został opracowany przez grupę roboczą „WG27K" współpracującą z DIGITAL SME. Grupa robocza „WG27K" składa się z ekspertów specjalizujących się w kwestiach standaryzacji w dziedzinie zarządzania bezpieczeństwem informacji oraz w pełni rozumiejących potrzeby MŚP w tym obszarze. Eksperci zostali desygnowani przez organizacje zrzeszające MŚP z różnych krajów UE, a ich wybór został dokonany na podstawie posiadanych przez nich kompetencji w celu zapewnienia zróżnicowanego składu grupy.

SBS oraz DIGITAL SME są jedynymi podmiotami posiadającymi prawa autorskie do darmowego i publicznie dostępnego poradnika w jego wersji oryginalnej dostępnej na stronie: https://www.sbs-sme.eu/.

Wydanie polskie publikacji zostało przygotowane przez Instytut Kościuszki za zgodą autorów.

SPIS TREŚCI

1 WPROWADZENIE DO CYBERBEZPIECZEŃSTWA

Współcześnie informacja stanowi podstawowy wytwór pracy dla większości organizacji, a dla wielu – nawet jedyny. Pozostałe organizacje są mocno uzależnione od przetwarzania informacji w celach biznesowych.

Niestety są też osoby mające złe zamiary, próbujące wykorzystać „uzależnienie" od informacji dla własnych celów. Niedawno obserwowaliśmy wiele przykładów ich nielegalnej działalności w postaci ataków wirusów typu ransomware (WannaCry, Petya), wycieków danych osobowych z wielkich korporacji (Equifax) czy wycieków dotyczących narzędzi szpiegowskich wykorzystywanych przez agencje wywiadowcze.

Wraz ze wzrostem liczby zagrożeń organizacje są zobowiązane do tego, by częściej zastanawiać się nad sposobami ochrony informacji, którymi dysponują, na przykład poprzez zastosowanie następujących prostych zabezpieczeń technicznych:

- zabezpieczanie dostępu do komputerów i systemów za pomocą haseł;
- instalowanie oprogramowania antywirusowego na komputerach użytkowników końcowych i serwerach;
- uniemożliwianie korzystania z pamięci USB wewnątrz organizacji; lub
- nabywanie coraz bardziej zaawansowanych i kosztownych rozwiązań.

Podczas gdy wiele z tych sposobów skutecznie chroni systemy, inne całkowicie marnotrawią zasoby finansowe i ludzkie. Nie oznacza to, że wspomniane wyżej narzędzia są złe czy nieskuteczne. Główny problem polega na podjęciu decyzji o tym, jakie narzędzia wybrać, określić ich koszt oraz jak skutecznie je wdrożyć, by spełniały potrzeby biznesowe organizacji.

PO CO PORADNIK DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW (MŚP)?

- **MŚP stanowią większość przedsiębiorstw w Europie. Przewyższają liczebnie duże korporacje i zatrudniają więcej ludzi. Uznaje się je także za siłę napędzającą innowacje w Europie.**
- **Większość MŚP nie doszacowuje poziomu ryzyka związanego z cyberatakami uważając, że informacje, jakimi dysponują, nie są na tyle cenne, by je kraść.**
- **W porównaniu z indywidualnymi użytkownikami małe przedsiębiorstwa posiadają dużą ilość aktywów cyfrowych i często mniejszą ilość zabezpieczeń niż duże organizacje.**

Z uwagi na złożoność środowiska informacyjnego oraz zawiłości związane z przepływem informacji, wiele organizacji rozumie obecnie potrzebę posiadania wykwalifikowanego personelu, tj. menadżerów bezpieczeństwa informacji, specjalistów cyberbezpieczeństwa oraz zespołów ds. bezpieczeństwa IT. Niektóre z nich tworzą odrębne działy odpowiedzialne za bezpieczeństwo informacji i reagowanie na incydenty cyberbezpieczeństwa. Mimo to wiele organizacji wciąż waha się, czy warto inwestować w środki bezpieczeństwa.

Luki w cyberbezpieczeństwie mogą prowadzić do poważnych problemów, które można podzielić na trzy główne kategorie:

- utrata dostępności danych, zakłócająca działalność biznesową;
- utrata poufności danych, szkodząca reputacji organizacji lub grożąca konsekwencjami prawnymi;
- utrata integralności prowadząca do wykorzystania nieprawidłowych lub nawet zafałszowanych danych.

Cyberbezpieczeństwo jest kluczowe dla ochrony aktywów firm niezależnie od wielkości i rodzaju działalności, jaką prowadzą. Czym dokładnie jest jednak cyberbezpieczeństwo?

DEFINICJA CYBERBEZPIECZEŃSTWA

Formalnie nie istnieje definicja **cyberbezpieczeństwa**, ale znaczenie tego terminu jest zbliżone do **bezpieczeństwa informacji**. Często uważa się, że cyberbezpieczeństwo obejmuje najbardziej techniczne aspekty dotyczące bezpieczeństwa informacji, które samo ma na celu ochronę informacji gromadzonej w formie papierowej, elektronicznej czy nawet tej przechowywanej przez ludzi. Cyberbezpieczeństwo dotyczy głównie ochrony i procesu przetwarzania informacji przechowywanych w postaci elektronicznej. Definiuje się je jako stan, w którym ryzyka związane z korzystaniem z technologii informatycznych, biorąc pod uwagę wszelkie zagrożenia i podatności, są zminimalizowane do akceptowalnego poziomu poprzez zastosowanie właściwych środków. Czynnik ludzki, w tym interesy narodowe, również odgrywają coraz ważniejszą rolę w cyberbezpieczeństwie. Stąd też cyberbezpieczeństwo obejmuje wykorzystanie odpowiednich środków w celu ochrony poufności, integralności oraz dostępności informacji oraz technologii informatycznych.

TERMINY I DEFINICJE

W celu lepszego zrozumienia tego poradnika, poniżej znajdują się definicje najpowszechniejszych terminów:

AKTYWA
Rzecz lub obiekt, który ma wartość dla organizacji. Istnieją różnego rodzaju aktywa, np. dane, sprzęt komputerowy, oprogramowanie, dostawcy usług, kadra czy fizyczne lokalizacje (siedziby) firmy.

ATAK
Umyślne wywołanie stanu zagrożenia; niepożądana lub nieuzasadniona czynność mająca na celu uzyskanie przewagi operacyjnej lub wyrządzenie szkody osobom trzecim poprzez działanie obierające sobie za cel zespół aktywów.

DOSTĘPNOŚĆ
Cecha polegająca na byciu osiągalnym i nadającym się do użytku na żądanie uprawnionego podmiotu.

POUFNOŚĆ
Cecha polegająca na udostępnianiu lub ujawnianiu informacji jedynie osobom, podmiotom czy procesom posiadającym odpowiednie uprawnienia.

KONTROLA
Sposób na zmniejszenie ryzyka. Zabezpieczenia obejmują procesy, procedury, urządzenia, praktyki lub inne działania, które skutecznie modyfikują ryzyko.

INTEGRALNOŚĆ
Cecha charakteryzująca się dokładnością oraz kompletnością.

BEZPIECZEŃSTWO INFORMACJI
Zachowanie poufności, integralności i dostępności informacji.

RYZYKO (w kontekście bezpieczeństwa informacji)
Ryzyko bezpieczeństwa informacji określa możliwość wykorzystania przez zagrożenia luk w zabezpieczeniach zasobów informacyjnych i tym samym wyrządzenia szkody organizacji.

OCENA RYZYKA (w kontekście bezpieczeństwa informacji)
Proces identyfikacji, analizy i oceny ryzyka.

POSTĘPOWANIE Z RYZYKIEM (w kontekście bezpieczeństwa informacji)
Proces modyfikacji ryzyka; zazwyczaj obejmuje unikanie ryzyka, dzielenie ryzyka, minimalizowanie ryzyka lub akceptację ryzyka.

ZAGROŻENIE
Potencjalna przyczyna niechcianego incydentu, który w efekcie może przynieść szkody.

PODATNOŚĆ
Słabość aktywów lub zabezpieczeń, która może być wykorzystana przez jedno lub więcej zagrożeń.

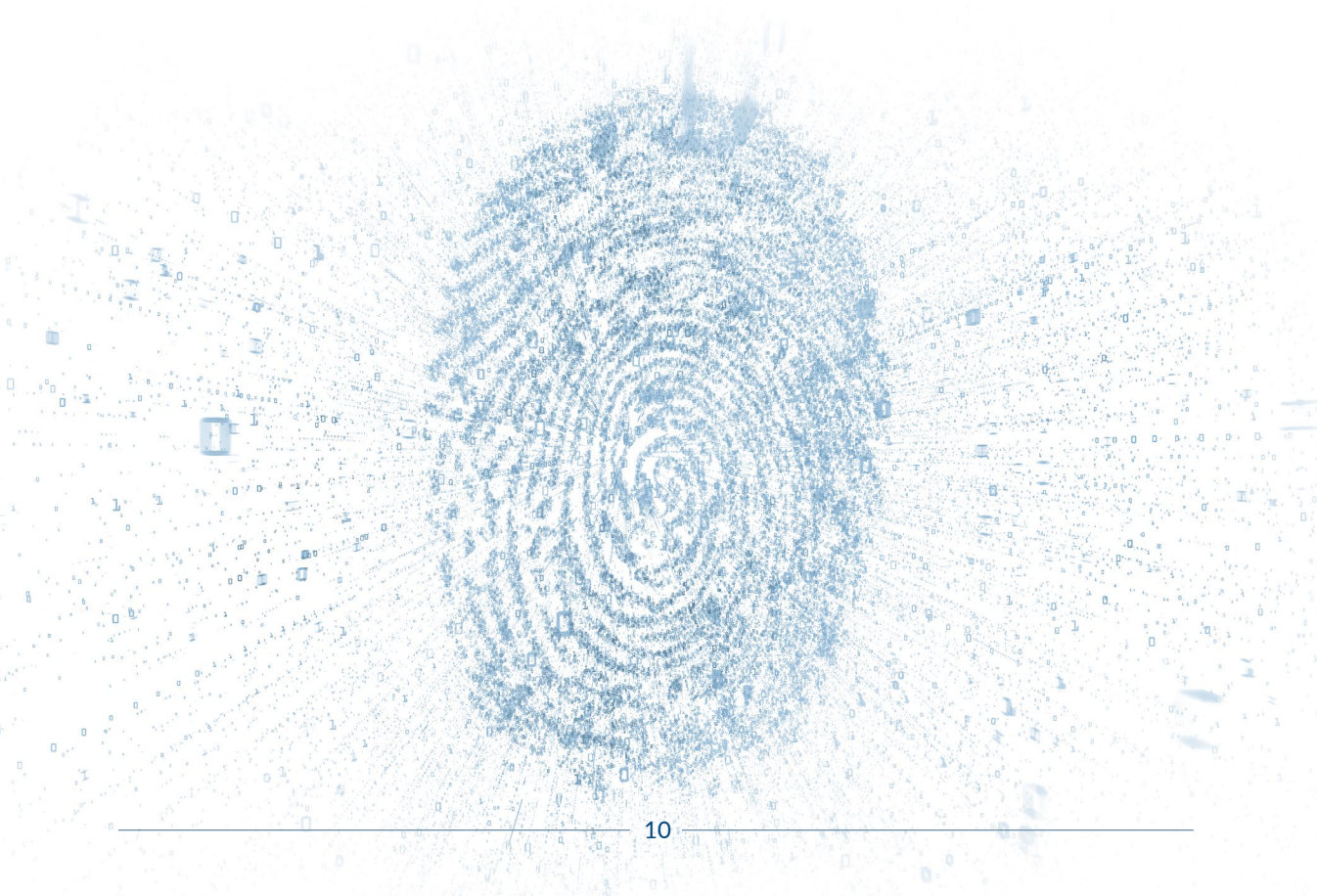
2 ZAKRES

Niniejszy poradnik jest skierowany do MŚP, których działalność biznesowa opiera się na zasobach technologicznych. Jego wytyczne mogą być z powodzeniem wdrażane przez inne organizacje niezależnie od ich wielkości czy stopnia złożoności.

Niniejszy poradnik przedstawia szereg praktycznych działań bazujących na standardzie ISO/IEC 27001, które w sposób znaczący mogą pomóc w stworzeniu systemu lub podniesieniu poziomu bezpieczeństwa informacji w MŚP. Pozwoli to na wzmocnienie ich działalności biznesowej oraz ułatwi nawiązywanie współpracy na rynkach lokalnych i unijnych.

Wszystkie wymienione działania zapewniają właściwe zarządzanie cyklem życia bezpieczeństwa informacji w obrębie organizacji.

Obejmuje ono stworzenie, planowanie, wdrażanie, obsługiwanie i usprawnianie wszystkich powiązanych ze sobą procesów w oparciu o kulturę ryzyka oraz koncepcję ciągłego doskonalenia.



3 ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI W MŚP

KROK 1: OKREŚL PODSTAWOWE ELEMENTY BEZPIECZEŃSTWA INFORMACJI

Zarządzanie bezpieczeństwem informacji ma wiele wspólnego z innymi głównymi inicjatywami, w które organizacje mogą się angażować. Zanim podejmie się jednak działania, warto zdecydować, jaką formę mają one przyjąć, w jakie ramy czasowe się wpisać oraz jakie zaangażowanie kadry jest wymagane. Wśród głównych inicjatorów powinien znaleźć się ekspert w danej dziedzinie oraz kadra kierownicza wyższego szczebla, którzy stworzą podwaliny pod wszystkie pozostałe działania.

Realizacja tego pierwszego kroku wymaga zaangażowania kadry kierowniczej wyższego szczebla, która powinna odpowiadać za stworzenie podstaw bezpieczeństwa informacji. Osobą, na której spoczywa odpowiedzialność za wykonanie tego zadania, jest menadżer bezpieczeństwa informacji. Właściciele systemu oraz informacji powinni również być informowani na bieżąco o postępach w realizacji zadania. Poniżej zamieszczamy szczegółowy opis członków kadry MŚP, którym można przypisać rolę w bezpiecznym zarządzaniu informacją.

Krok 1.1 Przydziel role i obowiązki

Odpowiednie przypisanie ról i obowiązków jest nieodzowne w każdym biznesie i w każdym podejmowanym działaniu. Start-upy czy małe organizacje często postrzegają bezpieczeństwo informacji jako samoistny proces, który nie jest uzależniony od poziomu ich zaangażowania. Niektóre wydają się je kompletnie ignorować.

Ważne jest, by decydując o podjęciu środków w celu zdefiniowania lub skorygowania systemu zarządzania bezpieczeństwem informacji w organizacji, również zdefiniować i nadać formalny charakter rolom i obowiązkom zanim przejdzie się do kolejnych etapów. Wszystkie późniejsze kroki mają przypisane w nawiasach „typowe funkcje osób" zgodne z macierzą odpowiedzialności RACI (ang. *Responsible* – Odpowiedzialny, *Accountable* – Nadzorujący, *Consulted* – Konsultowany, *Informed* – Informowany).

Niniejszy akapit zawiera ogólny opis najważniejszych ról oraz powiązanych z nimi obowiązków w obszarze zarządzania bezpieczeństwem informacji. Warto zauważyć, że mniejsze

organizacje mogą powierzyć jednej osobie więcej niż jedną rolę lub nawet zlecić te role podmiotowi zewnętrznemu (za wyjątkiem obowiązków kadry kierowniczej wyższego szczebla). Każda organizacja musi wyraźnie i formalnie przypisywać role i obowiązki w systemie bezpieczeństwa informacji zgodnie z własną strukturą i kulturą, co jest warunkiem wstępnym wdrożenia zaleceń niniejszego poradnika.

Kadra kierownicza wyższego szczebla

Ostateczna odpowiedzialność za bezpieczeństwo informacji spoczywa na kadrze kierowniczej wyższego szczebla, która jest częścią ogólnego systemu zarządzania. Głównym zadaniem kadry kierowniczej jest dopilnowanie, by bezpieczeństwo informacji służyło osiąganiu celów biznesowych poprzez skoordynowanie jego wymogów z dostarczaniem wartości przez organizację, właściwe zarządzanie aktywami i ustalenie odpowiadających mu kryteriów pomiaru osiąganych wyników. Kadra kierownicza wyższego szczebla nie musi wiedzieć o wszystkich aktywach w obrębie swojej organizacji, ale powinna mieć ogólne rozeznanie, jeśli chodzi o jej aktywa krytyczne oraz ich znaczenie dla działalności biznesowej.

W zależności od struktury danej organizacji kadra kierownicza wyższego szczebla obejmuje dyrektora wykonawczego (ang. Chief Executive Officer, CEO), dyrektora operacyjnego (ang. Chief Operating Officer, COO) lub zarząd. W celu optymalnego wykorzystania niniejszego poradnika należy zdecydować, kto musi przyjąć na siebie powyższe role.

PRACOWNICY PRZYPISANI DO RÓŻNYCH RÓL ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI ISTOTNYCH DLA ORGANIZACJI POWINNI PISEMNIE POTWIERDZIĆ SWOJE OBOWIĄZKI I ZADANIA.

Macierz RACI może okazać się pomocna przy przydzielaniu obowiązków i obejmować następujące zadania:

- określenie wymogów i klasyfikacji dotyczących bezpieczeństwa informacji;
- dokumentowanie wyników oceny ryzyka;
- zdefiniowanie, wdrożenie i utrzymanie środków bezpieczeństwa;
- akceptację ryzyka rezydualnego;
- sporządzanie dokumentacji dotyczącej systemu bezpieczeństwa (norm, procedur itd.);
- tworzenie i aktualizacja polityki bezpieczeństwa;
- monitorowanie systemu bezpieczeństwa;
- tworzenie planów dotyczących poprawy bezpieczeństwa;
- zwiększanie świadomości i przygotowanie planów szkoleń;
- przygotowanie planów ciągłości działania.

Do każdego z powyższych zadań należy przypisać następujące role i wynikające z nich obowiązki:

Komitet sterujący ds. bezpieczeństwa informacji

W określonych przypadkach MŚP mogą powołać komitet sterujący ds. bezpieczeństwa informacji złożony z pracowników wszystkich głównych pionów organizacji. Do dobrych praktyk należy stworzenie statutu komitetu, który służy głównie jako narzędzie do osiągnięcia konsensusu wśród głównych decydentów. Komitet sterujący ds. bezpieczeństwa informacji może pracować z kadrą kierowniczą wyższego szczebla i być odpowiedzialnym za działania związane z audytem i monitorowaniem.

Powołując do życia komitet sterujący ds. bezpieczeństwa informacji warto zaangażować w jego prace osoby bezpośrednio raportujące kadrze kierowniczej wyższego szczebla i ustalić kwartalny harmonogram spotkań. Komitet powinien spotykać się, by zająć się kwestiami związanymi z bezpieczeństwem informacji, takimi jak:

- zatwierdzanie norm i procedur bezpieczeństwa;
- przegląd analizy ryzyka oraz planu postępowania z ryzykiem;
- wyniki audytów i powiązane z nimi działania;
- monitorowanie planu bezpieczeństwa informacji;
- cel bezpieczeństwa informacji oraz kluczowe wskaźniki efektywności;
- wiedza oraz planowanie sesji szkoleniowych;
- reagowanie kryzysowe.

Oficer/Menadżer bezpieczeństwa informacji

Pomimo, iż bezpieczeństwo informacji dotyczy każdego pionu organizacji, coraz powszechniejsze staje się zatrudnianie menadżera bezpieczeństwa informacji, którego zadaniem jest koordynowanie odpowiednich działań. Rolę tę może pełnić dowolny odpowiednio umocowany członek kadry zarządzającej, np. menadżer IT lub dyrektor ds. technologii (CTO), posiadający wiedzę w zakresie przepływu informacji.

Ponieważ bezpieczeństwo informacji rzadko uznaje się za ogólną dyscyplinę zarządzania, to menadżer bezpieczeństwa informacji zazwyczaj udziela kadrze kierowniczej wyższego szczebla wskazówek dotyczących głównych jego aspektów przed przyjęciem strategii bezpieczeństwa informacji. Zaangażowanie kadry kierowniczej wyższego szczebla jest ważnym elementem bezpieczeństwa informacji. Jednym z kluczowych działań w tym względzie jest uzgodnienie celów biznesowych oraz tych dotyczących bezpieczeństwa informacji. Do pozostałych obowiązków oficera/menadżera bezpieczeństwa informacji często zalicza się:

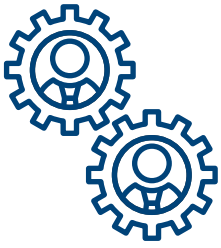
- ustalanie budżetów;
- wykorzystanie modeli ryzyka i korzyści do oceny i postępowania z ryzykiem;
- opracowanie polityk i procedur dotyczących bezpieczeństwa informacji;
- przegląd wyników działań monitorujących.

Oficer/menadżer bezpieczeństwa informacji jest zazwyczaj odpowiedzialny za działania na rzecz zwiększania świadomości na temat bezpieczeństwa informacji, w tym ustanowienie kanałów komunikacji i raportowania. Sprawne działanie systemu bezpieczeństwa informacji zależy w dużym stopniu od komunikacji, zarówno tej wewnętrznej jak i zewnętrznej.

Oficer/menadżer bezpieczeństwa informacji pełni kluczową rolę, w zakresie wdrażania zaleceń niniejszego poradnika, dlatego wybór osoby na to stanowisko powinien opierać się na jej kompetencjach i doświadczeniu w tej dziedzinie. Profil kandydatów, jeśli wybiera się ich pod kątem tej konkretnej roli, może obejmować wachlarz funkcji, od menadżera bezpieczeństwa do dyrektora bezpieczeństwa informacji (CISO). Więcej szczegółów na temat profili zawodowych oraz związanych z nimi kompetencjami można znaleźć w porozumieniu roboczym CEN (CWA 16458) dotyczącym europejskich profili zawodowych w sektorze ICT.

ZALETY POWOŁANIA KOMITETU DS. BEZPIECZEŃSTWA INFORMACJI:

Ściślejsza współpraca pomiędzy różnymi obszarami w organizacji



Skuteczniejsze rozpowszechnianie kultury bezpieczeństwa informacji dzięki bezpośredniemu zaangażowaniu większej liczby wydziałów

Lepszy ogląd sytuacji przy podejmowaniu decyzji, ponieważ wszystkie istotne obszary podlegają komitetowi

Ustalanie rutynowej procedury przeglądu i kontroli statusu bezpieczeństwa informacji i rozwoju

POWOŁUJĄC KOMITET DS. BEZPIECZEŃSTWA INFORMACJI NALEŻY WZIĄĆ POD UWAGĘ NASTĘPUJĄCE KWESTIE:

- Każdy dział powinien być reprezentowany przez właściwy organ decyzyjny, aby uniknąć braku równowagi między różnymi działami
- Porządek spotkania należy z wyprzedzeniem zaplanować i rozesłać
- Spotkania powinny odbywać się systematycznie i okresowo, np. co trzy miesiące
- Należy ustalić reguły prowadzenia spotkań, w tym wszelkie decyzje dotyczące tego, kto prowadzi spotkania i jak uczestnicy będą rozwiązywać potencjalne konflikty
- Komitet powinien podejmować istotne decyzje dotyczące bezpieczeństwa informacji
- Należy przestrzegać harmonogramu

Właściciele systemu i informacji

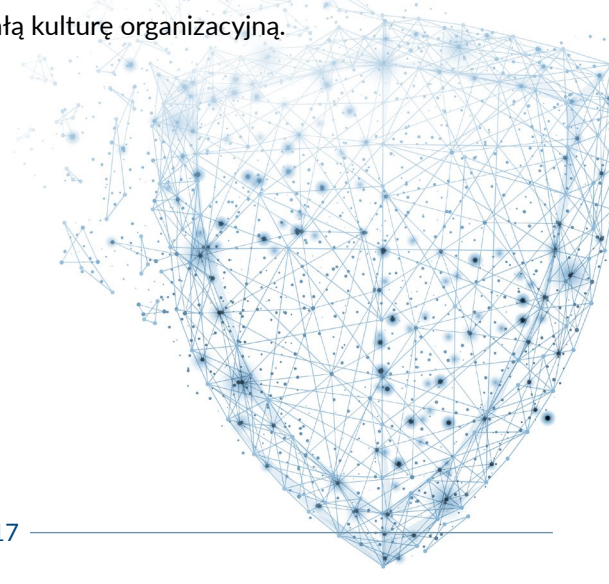
Bardziej ustrukturyzowane organizacje mogą być zmuszone do wskazania szeregu osób do wykonywania bieżących zadań, w celu ochrony systemów informacyjnych, które kontrolują. To oni są „właścicielami systemu". Jednocześnie właściciele firmy odpowiedzialni za procesy i dane powinni być zaangażowani w proces definiowania wymagań dla ich ochrony, niezależnie od systemów informatycznych. To oni są „właścicielami informacji". Zarówno właściciele systemu jak i informacji powinni pomagać organizacji poprzez zapewnienie funkcjonowania oraz prawidłowego działania zabezpieczeń w obszarze bezpieczeństwa informacji.

Zazwyczaj właściciele mają prawo do wprowadzania zmian w obszarach, które do nich należą np. ulepszenia systemu, wprowadzania ułatwień itd. Jednakże decyzje te powinny zawsze uwzględniać wpływ na bezpieczeństwo informacji. Aby ten model zadziałał, musi być jasne, kim są właściciele systemu i informacji w organizacji. Rozgraniczenie tych ról powinno odbywać się z udziałem menadżera IT oraz dyrektora operacyjnego (COO). Organizacja może często mieć trudności ze znalezieniem właścicieli systemów i informacji na niższych szczeblach hierarchii zarządzania, a więc ludzi, którzy decydują o zwiększaniu zasobów lub wprowadzaniu ułatwień. Rozwiązanie to wymaga delegowania praktyk decyzyjnych i spójnej kultury organizacyjnej.

Kadra

Sprawne działanie systemu bezpieczeństwa informacji zależy od odpowiedniego przeszkolenia i wykształcenia personelu. Pracownicy i kontrahenci powinni mieć pełną świadomość przyczyn istnienia środowiska kontroli wokół nich, aby mogli utrzymać bezpieczeństwo informacji na odpowiednim poziomie i nie narażać go na szwank.

Pracownicy i kontrahenci powinni umieć rozpoznać nietypowe zachowanie oraz niezwłocznie zgłaszać wszelkie wątpliwości menadżerowi bezpieczeństwa informacji w celu zminimalizowania strat po stronie organizacji. Dosyć często to właśnie pracownicy oraz kontrahenci są celem ataków, dlatego posiadanie odpowiednio wykształconej kadry wzmacnia w sposób znaczący ogólne środowisko bezpieczeństwa informacji. To tacy pracownicy mogą również być w stanie przekształcić tę wiedzę i doświadczenie w trwałą kulturę organizacyjną.



KROK 2: UŚWIADOM SOBIE, CO NALEŻY CHRONIĆ

Od tego rozdziału, do opisów poszczególnych zadań, które mają na celu ułatwić bezpieczne zarządzanie informacją w organizacji, dołączone zostaną przykłady, np. rysunki, tabele itp. Przykłady te pomogą czytelnikowi zrozumieć ten poradnik.

Przed zastosowaniem jakiegokolwiek środka bezpieczeństwa informacji, organizacja musi uzyskać wstępny obraz tego, które składniki majątku mają dla niej największą wartość. Te składniki majątku, zazwyczaj określane mianem aktywów, można ogólnie zaklasyfikować jako rodzaj informacji (patrz Krok 2.1), wśród których można wyróżnić aktywa niematerialne oraz inne aktywa (patrz Krok 2.2), które mają zazwyczaj charakter materialny.

Głównym celem tej czynności jest wskazanie kluczowych aktywów, które są pod kontrolą organizacji i które wymagają ochrony. Jest to szczególnie ważne przy określaniu relacji między aktywami oraz przy określaniu obowiązków.

Role, których zazwyczaj się to tyczy: kadra kierownicza wyższego szczebla (A), właściciele informacji (C), właściciele systemu (C), oficer/menadżer bezpieczeństwa informacji (R).

Krok 2.1 Określ typ informacji

Określenie typu informacji jest ważne przy budowie **mapy aktywów**, zaczynając od aktywów niematerialnych – czyli informacji posiadanych przez organizację.

Podejście odgórne

Organizacja może zdecydować się na przyjęcie „odgórnego“ podejścia, w którym informacje (białe zaokrąglone prostokąty poniżej) określane są w momencie ich przepływu między procesami (kolorowe zaokrąglone prostokąty poniżej).

Rysunek 1: Przykład mapy aktywów w odniesieniu do hipotetycznych informacji w ramach danej organizacji

W celu jak najlepszego wykorzystania podejścia oddolnego, organizacja powinna dobrze poznać swoje procesy, np. zdawać sobie sprawę z ich natury, wiedzieć, kto jest odpowiedzialny za każdy proces itd. Związek pomiędzy działaniami organizacji a informacją można wyjaśnić zaczynając od spojrzenia na procesy „z lotu ptaka" i stopniowego schodzenia w dół, aż do identyfikacji zasobów informacyjnych. Właściciele informacji (zazwyczaj menadżerowie lub kierownicy działów) są najbardziej odpowiednimi osobami do klasyfikacji i oceny znaczenia tych informacji wewnątrz organizacji. Warto przeprowadzić krótki wywiad z każdym z właścicieli informacji w celu uzyskania pełnego obrazu danych, jakimi zarządza organizacja.

Wykorzystanie prostych schematów procesu pomaga określić i przedstawić różne typy informacji, którymi zarządza organizacja w podejściu odgórnym.

Podejście oddolne

Podejście odgórne wymaga bardzo dobrego zrozumienia procesów organizacyjnych. Z kolei podejście oddolne może być stosowane w każdej organizacji, niezależnie od poziomu jej dojrzałości. Przy wdrażaniu podejścia oddolnego doskonałym punktem wyjścia jest odpowiedź na pytanie: „Jakimi informacjami ogólnie rzecz ujmując dysponuje organizacja?" To pytanie można zadać osobie lub osobom posiadającym całościowy obraz tego, co się dzieje w organizacji. Poniższa prosta lista przedstawia najważniejsze dane, które należy wziąć pod uwagę:

a. dane osobowe (np. nazwiska, adresy, numery PESEL, informacje o wynagrodzeniach);
b. wrażliwe dane osobowe (np. diagnozy lekarskie, poglądy polityczne, dane dotyczące płatności kartą);
c. strategiczne dane przedsiębiorstwa (np. biznesplany, prognozy, wstępne sprawozdania budżetowe);
d. dane projektowe (np. projekt produktu, własnościowy kod źródłowy);
e. inne dane przedsiębiorstwa (np. dane z monitoringu, statystyki produkcyjne, dane podatkowe).

ORGANIZACJE MOGĄ JEDNOCZEŚNIE WYKORZYSTYWAĆ PODEJŚCIE ODGÓRNE I ODDOLNE, PONIEWAŻ OBA MAJĄ SWOJE WADY I ZALETY

Podejście odgórne jest bardziej uproszczone i pokazuje zależność przyczynowo-skutkową, ale może stwarzać problemy przy kompilacji całościowej mapy obejmującej również procesy

Podejście oddolne wymaga mniejszej wiedzy lub dojrzałości organizacyjnej, ale jest mniej dokładne, gdyż nie łączy informacji z żadną koncepcją biznesową

Po stworzeniu mapy aktywów organizacja powinna dobrze znać swoje aktywa informacyjne na płaszczyźnie koncepcyjnej, niezależnie od tego, z jakiego sprzętu korzysta do ich przechowywania lub przetwarzania.

Krok 2.2 Określ pozostałe aktywa

Wskazana informacja może być przechowywana, przetwarzana lub przesyłana przy użyciu kilku innych aktywów, głównie (ale nie wyłącznie) technologicznych. Aktywa te zwykle stanowią warstwy oprogramowania, które działają w systemach informatycznych, ale mogą do nich również należeć dokumenty w formie papierowej i dyski lub usługi świadczone przez usługodawców zewnętrznych. Podejście oddolne zazwyczaj pomaga prawidłowo je zidentyfikować, angażując do tego pracowników działu IT i administratorów (niezależnie od tego, czy oficjalnie wyznaczono ich jako właścicieli systemu). Zaleca się, aby nie pomijać kluczowych aktywów, które należą do następujących kategorii:

1. urządzenia końcowe (laptopy, komputery stacjonarne, tablety, smartfony), serwery i sprzęty;
2. oprogramowanie użytkownika końcowego (nie licząc pakietów oprogramowania do automatyzacji prac biurowych lub systemów operacyjnych);
3. usługodawcy (w tym dostawcy usług HR, usług sieciowych i rozwiązań w chmurze);
4. personel (pracownicy zatrudnieni bezpośrednio przez firmę i pracownicy-podwykonawcy);
5. lokalizacje fizyczne (posiadane biura i sale komputerowe).

Jak zostało to opisane w poprzednim kroku, elementy te mogą również być wstępnie badane w odgórnej interakcji z właścicielami informacji, bezpośrednio po zdefiniowaniu informacji związanych z procesami i dopracowaniu ich z właścicielami systemu. Opierając się na powyższym przykładzie, taka ustrukturyzowana lista może wyglądać w następujący sposób:

OPROGRAMOWANIE	SPRZĘT KOMPUTEROWY	KADRA	DOSTAWCY	LOKALIZACJE
Aplikacja CRM	Serwery produkcyjne	Personel wewnętrzny	Dostawca chmury	Główne biura
Aplikacja ERP	Serwery testowe		Dostawca TLC	
Udostępnione foldery	Komputery pracowników			
	Smartfony pracowników			

Rysunek 2: Przykład mapy aktywów określającej kluczowe aktywa inne niż informacja w ramach danej organizacji

Krok 2.3 Określ związek pomiędzy informacją a pozostałymi aktywami

Gdy wszystkie kluczowe aktywa zostaną jasno zdefiniowane, ustalenie, które z nich są powiązane z określonymi informacjami, jest prostym, ale skutecznym sposobem ułatwiającym zrozumienie tego, które informacje i aktywa wymagają ochrony, a następnie, w jakim stopniu je chronić. W tym celu można stworzyć prostą macierz, jak ta załączona poniżej. Wypełnione komórki wskazują związek między aktywami a informacją; puste komórki oznaczają brak powiązania.

	Dane ogólne klienta	Roszczenia klienta	Kod źródłowy	Specyfikacje projektowe	Zapytania ofertowe
Aplikacja CRM					
Serwery produkcyjne					
Serwery testowe					
Komputery pracowników					
Smartfony pracowników					
Udostępnione foldery					
Aplikacja ERP					
Personel wewnętrzny					
Dostawca chmury					
Dostawca TLC					
Główne biura					

Tabela 1: Przykład macierzy określającej związek pomiędzy informacją a pozostałymi aktywami

Z chwilą, gdy wszystkie te związki zostaną jasno ustalone, mapa aktywów jest ukończona. Będzie ona bardzo pomocna w kolejnych krokach. Oczywiście, można zebrać większą ilość informacji dla każdego z aktywów, do momentu stworzenia kompletnego inwentarza, który można wykorzystać, by lepiej nimi zarządzać. Należy pamiętać, że mapa aktywów musi być stale aktualizowana. W przeciwnym razie jej użyteczność szybko spadnie.

KROK 3: OCEŃ RYZYKA ZWIĄZANE Z BEZPIECZEŃSTWEM INFORMACJI

Ocena ryzyka bezpieczeństwa informacji koncentruje się na wczesnym ustaleniu czynników mogących mieć negatywny wpływ na aktywa, przepływ środków pieniężnych, zobowiązania prawne lub wizerunek danej organizacji. Ten etap jest kluczowy dla zrozumienia zagrożeń, przed którymi stoi organizacja tak, aby mogła ona wdrożyć odpowiednie zabezpieczenia w celu ich uniknięcia, powstrzymania lub zapewnienia powrotu do działania po ich wystąpieniu. Dokonując priorytetyzacji ryzyk każda organizacja może skoncentrować swoje aktywa obronne tam, gdzie ryzyka mogą spowodować największe straty, co ostatecznie doprowadzi do optymalnej skuteczności wykorzystania tych aktywów.

Role, których zazwyczaj to dotyczy: kadra kierownicza wyższego szczebla/komitet sterujący ds. bezpieczeństwa informacji (A), właściciele informacji (C), właściciele systemu (C), oficer/menadżer bezpieczeństwa informacji.

Krok 3.1 Określ wartość aktywów

W celu pełnego dopasowania mapy aktywów (patrz Krok 2.3) do procesu oceny ryzyka, należy dodać jeden kluczowy element: ocenę znaczenia każdego z aktywów w obrębie organizacji.

Najprostszym sposobem, aby dokonać takiej oceny, jest rozpoczęcie od określonej informacji i rozważenie co najmniej dwóch spośród głównych cech związanych z bezpieczeństwem informacji: dostępności i poufności. Można je uzupełnić o integralność, ale w najprostszych sytuacjach można tę cechę traktować jako ściśle związaną z dostępnością. Każdy właściciel informacji powinien dokonać podstawowej oceny informacji określonej w Kroku 2.1 za pomocą poniższej tabeli stanowiącej punkt odniesienia i przypisać wartości dla dostępności i poufności dla każdego zidentyfikowanego elementu informacji.

	Wartość niska	Wartość wysoka
Dostępność (A)	Czy niedostępność tej informacji mogłaby mieć znaczący wpływ na działalność biznesową lub reputację organizacji?	
	Nie	**Tak**
Poufność (C):	Czy nieautoryzowane rozpowszechnienie tej informacji może spowodować istotny uszczerbek dla konkurencyjności organizacji lub naruszać podstawowe zobowiązania prawne lub kontraktowe?	
	Nie	**Tak**

Tabela 2: Ocena aktywów pod kątem ich dostępności i poufności

Zastosowanie powyższej tabeli do tego przykładu mogłoby skutkować następującymi wartościami:

Dane ogólne klienta	Roszczenia klienta	Kod źródłowy	Specyfikacje projektowe	Zapytania ofertowe	Dokumenty zamówień
A: niska C: wysoka	A: niska C: niska	A: niska C: wysoka	A: niska C: wysoka	A: wysoka C: niska	A: niska C: wysoka

Tabela 3: Przykład oceny informacji pod kątem jej dostępności i poufności

Ponieważ główne wartości wszystkich pozostałych aktywów są powiązane z informacjami, jakie przechowują, przetwarzają lub przekazują, ta początkowa ocena może być przejmowana przez wszystkie aktywa związane z ocenianą informacją na mapie aktywów. Oznacza to, że ich związek z najwyżej ocenianą informacją pokazuje ich prawdziwą wartość dla organizacji, jak pokazano poniżej.

	Dane ogólne klienta	Roszczenia klienta	Kod źródłowy	Specyfikacje projektowe	Zapytania ofertowe	
	A: niska C: wysoka	A: niska C: niska	A: niska C: wysoka	A: niska C: wysoka	A: wysoka C: niska	
Aplikacja CRM						A: niska C: wysoka
Serwery produkcyjne						A: wysoka C: wysoka
Serwery testowe						A: niska C: wysoka
Komputery pracowników						A: wysoka C: wysoka
Smartfony pracowników						A: niska C: wysoka
Udostępnione foldery						A: niska C: wysoka
Aplikacja ERP						A: wysoka C: niska
Personel wewnętrzny						A: wysoka C: wysoka
Dostawca chmury						A: wysoka C: wysoka
Dostawca TLC						A: wysoka C: wysoka
Główne biura						A: wysoka C: wysoka

Tabela 4: Przykłady macierzy kompleksowo identyfikującej związek między aktywami a ich oceną pod kątem dostępności i poufności

Tak wypełniona i ulepszona mapa aktywów, niezależnie od postaci, dostarcza odpowiedzi na pytanie, co i w jakim stopniu wymaga ochrony systemu bezpieczeństwa informacji, w zależności od rzeczywistej roli konkretnego aktywa.

Oceny aktywów można dokonywać przy pomocy różnego rodzaju skali (np. stosującej wartości niska, średnia lub wysoka). W celu zwiększenia efektywności takiej analizy, oddziaływanie można ocenić biorąc pod uwagę kryteria takie jak:

- **wymogi prawne**
- **interesy ekonomiczne lub handlowe**
- **reputację (publiczny wizerunek)**
- **bezpieczeństwo**

Krok 3.2 Dokonaj oceny kontekstu, w którym działa organizacja

Gruntowna znajomość środowiska, w którym działa organizacja, ma kluczowe znaczenie przy określaniu wymogów dotyczących bezpieczeństwa informacji. Agencja UE ds. Bezpieczeństwa Sieci i Informacji, ENISA, opracowała model zagrożeń dla cyberbezpieczeństwa, który jest użyteczny przy uwzględnianiu wszystkich prawdopodobnych zagrożeń stojących przed organizacją. Model ENISA wyszczególnia następujące kategorie zagrożeń:

a) katastrofy (np. trzęsienie ziemi, powódź, pożar);
b) przerwy (np. strajk, niedostępność niezbędnej usługi);
c) ataki fizyczne (np. kradzież, sabotaż);
d) naruszenie prawa (np. naruszenie przepisów, orzeczenia sądowego);
e) nieumyślne szkody (np. wyciek informacji, utrata urządzenia);
f) awarie, usterki (np. awaria lub usterka sprzętu komputerowego);
g) nieetyczne działania, nadużycia (np. malware, socjotechniki, ataki siłowe (ang. *brute force*));
h) podsłuchiwanie, przechwycenie, porwanie (np. szpiegostwo, atak MITM (ang. *man in the middle*)).

Ryzyko wystąpienia tych zagrożeń należy oceniać biorąc pod uwagę historyczne dane dotyczące takich zdarzeń (tam, gdzie są one dostępne) i doświadczenie kadry pracowniczej. Tego rodzaju ocena może pomóc w ustaleniu, jak poniższe warunki odnoszą się do środowiska, w którym działa organizacja:

1. Jak bardzo podatne są siedziby organizacji na wystąpienie klęsk żywiołowych lub zdarzeń losowych (powodzie, pożary, trzęsienia ziemi)?
2. Jak bardzo podatne są siedziby organizacji na wystąpienie przerw w dostawie usług (połączeń internetowych, utratę zasilania, strajki)?
3. Jak lojalny jest personel (mała rotacja kadr, brak niepokojów, spójność zespołów)?
4. Jak silny wpływ wywierają przepisy lub wymagania kontraktowe na działalność biznesową?
5. Jak bardzo podatna jest organizacja na popełnianie przez personel tzw. błędów ludzkich?
6. Jak bardzo działalność biznesowa jest zależna od dostawców zewnętrznych?
7. W jakim stopniu usługi ICT narażają organizację na zagrożenia płynące z Internetu?
8. Jak ważny jest wizerunek publiczny organizacji?

Właścicielami informacji i aktywów, odpowiednimi do udzielenia odpowiedzi na powyższe pytania mogliby być:

- **MENADŻER IT w następujących kategoriach: „nieumyślne szkody", „katastrofy", „awarie, usterki", „przerwy", „podsłuchiwanie, przechwycenie, porwanie", „nieetyczne działania, nadużycia"**
- **OFICER/ MENADŻER BEZPIECZEŃSTWA INFORMACJI LUB KIEROWNIK OBIEKTU w następujących kategoriach: „ataki fizyczne", „katastrofy", „awarie, usterki"**
- **MENADŻER DZIAŁU PRAWNEGO w kategorii „naruszenie prawa"**
- **MENADŻER DZIAŁU KADR w kategorii „przerwy"**

Odpowiedzi na te pytania (skutkujące wyborem wartości wysoka, niska lub brak), uzyskane w drodze konsultacji z odpowiednimi właścicielami informacji i aktywów, mogą pomóc w ustalaniu prawdopodobnych zagrożeń, z którymi organizacja będzie musiała się zmierzyć, odnoszącymi się bezpośrednio do modelu zagrożeń dla cyberbezpieczeństwa ENISA (1 do a, 2 do b itd.). Kwestie te powinny być rozważane oddzielnie w stosunku do środków bezpieczeństwa już wdrożonych w organizacji.

Niniejszy poradnik może zostać wykorzystany do radzenia sobie z grupami zagrożeń wykraczającymi poza te zdefiniowane przez agencję ENISA. Odpowiednie poszerzanie listy zagrożeń wymaga jedynie zmapowania zestawu zabezpieczeń.

Wszystkie zagrożenia, dla których odpowiedzi na pytania brzmią inaczej niż „brak", i które mają zastosowanie do któregokolwiek ze zidentyfikowanych aktywów opisanych w poniższej tabeli, należy traktować jako potencjalne przyczyny ryzyka dla organizacji.

	Katastrofy	Przerwy	Ataki fizyczne	Naruszenie prawa	Nieumyślne szkody	Awarie, usterki	Nieetyczne działania, nadużycia	Podsłuchiwanie, przechwytywanie, porwanie
Sprzęt komputerowy	x		x		x	x	x	
Oprogramowanie				x	x	x	x	x
Dostawcy usług		x		x		x		x
Kadra	x	x		x			x	x
Fizyczne lokalizacje	x		x					

Tabela 5: Przykład macierzy do oceny rodzaju kontekstu, w którym działa organizacja

Na przykład, jeśli odpowiedź na pytanie 3) brzmiała: wartość „niska", to odpowiadający zagrożeniu punkt c) atak fizyczny dotyczyłby aktywów sprzętowych i fizycznej lokalizacji. Na przykładowej mapie aktywów (Rysunek 2) byłyby to serwery produkcyjne, serwery testowe, komputery pracowników, smartfony pracowników i główne biura.

Krok 3.3 Określ, jakie zabezpieczenia zostały już wdrożone

Poziom bezpieczeństwa informacji jest zależny od wdrożonych zabezpieczeń, są one kluczowymi elementami odpowiedzialnymi za redukcję ryzyk. Jeśli odpowiednio się je wdraża, potrafią redukować ryzyko w znaczący sposób. Pewne zabezpieczenia są często już wdrożone w firmie. Niemniej powinny być one rozważane nie tylko na poziomie organizacji, ale w większości przypadków, także na poziomie aktywów. Pomoże to zidentyfikować wszelkie możliwe luki w systemie ochrony.

Załącznik A do normy ISO/IEC 27001 zawiera obszerną listę zabezpieczeń, stworzoną przede wszystkim po to, aby umożliwić organizacji sprawdzenie poziomu „kompletności" potencjalnych i możliwych do zastosowania zabezpieczeń. Lista ta została uproszczona dla potrzeb MŚP i dołączona jako **Załącznik A do niniejszego poradnika.** Zawiera on też odniesienia do oryginalnych zabezpieczeń umieszczonych w Załączniku A normy ISO/IEC 27001. Każde zabezpieczenie na liście powinno mieć oznaczenie mówiące o tym, czy zostało ono w pełni zastosowane czy nie (częściowe zastosowanie zostanie uznane za brak zastosowania) dla każdej grupy aktywów związanych z konkretną informacją.

KROK 4: BEZPIECZEŃSTWO INFORMACJI – ZAPROJEKTUJ, STOSUJ I MONITORUJ ZABEZPIECZENIA

Z chwilą, gdy organizacja stanie się w pełni świadoma tego, co powinna chronić i jak obecnie to robi, może zacząć podejmować decyzje dotyczące wdrażania i ulepszania nowych zabezpieczeń. Kadra kierownicza wyższego szczebla lub komitet sterujący ds. bezpieczeństwa informacji powinni ocenić, jakie działanie należy podjąć w celu ograniczenia konkretnego ryzyka oraz określić czas i fundusze przeznaczone na każde rozwiązanie. Większość propozycji zazwyczaj przedstawia oficer/menadżer bezpieczeństwa informacji. Wybrane zabezpieczenia powinny być efektywne zarówno pod względem działania jak i kosztów.

Role, których zazwyczaj to dotyczy: kadra kierownicza wyższego szczebla/komitet sterujący ds. bezpieczeństwa informacji (A), właściciele informacji (R), właściciele systemu (R), kadra (R), oficer/menadżer bezpieczeństwa informacji (R).

Krok 4.1 Określ zabezpieczenia, które należy wdrożyć i umieścić w Planie Bezpieczeństwa Informacji

Podjęcie decyzji o tym, które zabezpieczenia należy wdrożyć w konkretnym środowisku, jest najtrudniejszą decyzją w całym obszarze bezpieczeństwa informacji. Żadna kombinacja zabezpieczeń nie jest idealna w każdej sytuacji, gdyż ich unifikacja mogłaby doprowadzić do wyższych niż niezbędne koszty, a także do powstania licznych zabezpieczeń i incydentów, które są trudne do przewidzenia.

Zgodnie z poprzednimi krokami i dobrymi praktykami, niniejszy poradnik proponuje w Załączniku A podział zabezpieczeń na dwie główne kategorie:

1. **zabezpieczenia podstawowe** – najlepiej, by były wdrażane w każdej sytuacji;
2. **zabezpieczenia dodatkowe** – powinny być wykorzystywane do ochrony aktywów o znacznej wartości, narażonych na potencjalne zagrożenia.

Podstawowe zabezpieczenia zostały pogrupowane w pierwszej części Załącznika A (A.1) i, o ile nie wystąpią szczególne okoliczności, powinny być zawsze wdrażane. Załącznik X niniejszego poradnika przedstawia idealny przykład zabezpieczenia podstawowego, którym jest **polityka bezpieczeństwa informacji.** Finalna wersja polityki bezpieczeństwa informacji powinna zostać formalnie zatwierdzona przez kadrę kierowniczą wyższego szczebla.

Zabezpieczenia dodatkowe zostały pogrupowane w drugiej części Załącznika A (A.2). W tym wypadku każde zabezpieczenie dodatkowe jest powiązane z zagrożeniami, które niweluje

(zabezpieczenia zostały wymienione w trzeciej części Załącznika A (A.3)). Brak wartości w odpowiedniej komórce określającej zagrożenie w części A.3, oznacza, że zabezpieczenie nie niweluje go w znaczący sposób. Obecność wartości „wtórny" oznacza, że robi to w sposób odczuwalny. Natomiast obecność wartości „pierwotny" oznacza, że robi to w sposób skuteczny.

Nadanie każdemu z aktywów wartości w *Kroku 3.1* i pozwiązanie ich z właściwymi zagrożeniami w *Kroku 3.2* może pomóc użytkownikom w podjęciu decyzji o tym, czy należy zastosować zabezpieczenie czy też nie. Jeśli któryś z aktywów posiada wartość wysoką dla poufności lub dostępności **LUB** stanowi wysoce prawdopodobne zagrożenie, wtedy należy zastosować wyłącznie zabezpieczenia dodatkowe oznaczone jako „pierwotne" dla tego konkretnego zagrożenia. Jeśli któryś z aktywów posiada wartość wysoką dla poufności lub dostępności **ORAZ** stanowi wysoce prawdopodobne zagrożenie, wtedy warto rozważyć zastosowanie zabezpieczenia oznaczonego jako „wtórne" dla tego konkretnego zagrożenia.

Na przykład smartfony pracowników, których ocena w Tabeli 4 to „A: niska, C: wysoka", stanowią sprzęt, a tym samym są narażone na „niski" poziom zagrożenia fizycznym atakiem. Wszystkie zabezpieczenia, gdzie istnieje „pierwotny" związek z groźbą ataku fizycznego, będą miały zastosowanie do smartfonów pracowników, jak również do zabezpieczeń podstawowych. Oznacza to:

- A2.06 Zarządzanie nośnikami wymiennymi;
- A2.10 Bezpieczeństwo fizyczne;
- A2. 11 Ochronę przed zagrożeniami zewnętrznymi i środowiskowymi;
- A2.12 Konserwację sprzętu;
- A.2.16 Zapasowe kopie informacji.

Poradnik ten może być również stosowany w odniesieniu do innych zabezpieczeń niż te przedstawione w Załączniku A lub w momencie dodawania do niego nowych zabezpieczeń. W takim wypadku należy ponownie stworzyć mapę grupy zagrożeń.

Weryfikacja zastosowanych zabezpieczeń przedstawionych w poprzednim kroku oraz tych wyszczególnionych w wymionionych wyżej kategoriach powinna być przeprowadzana **na poziomie aktywów.**

Sytuacje, w których skuteczność istniejącego zabezpieczenia okazuje się być mniejsza niż zalecana lub go brakuje, powinny być odnotowane i poddane dalszej analizie.

Wykaz tego rodzaju zabezpieczeń stanowi podstawę do stworzenia **Planu Bezpieczeństwa Informacji,** który pozwoli organizacji udoskonalić ochronę bezpieczeństwa informacji w sposób selektywny.

Plan Bezpieczeństwa Informacji powinien zawierać więcej elementów niż wykaz zabezpieczeń. Może przykładowo obejmować szereg działań z przypisanymi im właścicielami, daty, koszty i inne informacje.

W praktyce może mieć formę arkusza z następującymi polami:

Kod	**Identyfikator**
Źródło	**Aktywność urządzenia źródłowego**
Opis działania	**Tekst opisowy**
Właściciel	**Funkcja lub osoba**
Przyczyna	**Powód aktywności**
Priorytet	**Niski**
Status	**Otwarty/Zamknięty**
% zaawansowania	**0%-100%**
Aktywa	**Koszty, personel**
Data rozpoczęcia	**dd-mm-rrrr**
Data zakończenia	**dd-mm-rrrr**
Uwagi	**Pozostałe adnotacje**

Tabela 6: Szablon do śledzenia działań realizowanych w ramach Planu Bezpieczeństwa Informacji

Krok 4.2 Zarządzaj Planem Bezpieczeństwa Informacji

Po zatwierdzeniu planu, oficer/menadżer bezpieczeństwa informacji powinien być odpowiedzialny za okresowe (np. miesięczne lub kwartalne) monitorowanie Planu Bezpieczeństwa Informacji, aby ocenić, czy przebiega on w sposób prawidłowy i czy angażuje w możliwie jak największym zakresie inne zainteresowane strony.

Monitoring ten powinien odbywać się za pośrednictwem posiedzeń oficjalnego komitetu (np. komitetu sterującego ds. bezpieczeństwa informacji). W trakcie takich spotkań wszyscy zaangażowani specjaliści powinni informować o swoich postępach, trudnościach i zmianach, które należy wprowadzić do planu.

Plan powinien być odpowiednio aktualizowany, a jeśli zostaną wprowadzone w nim istotne zmiany wymagające nowych środków, należy ponownie przedłożyć go do zatwierdzenia przez kadrę kierowniczą wyższego szczebla.

W przypadku braku znaczących zmian, plan powinien nadal być zatwierdzany okresowo przez kadrę kierowniczą wyższego szczebla (co najmniej raz do roku, w miarę możliwości przed zatwierdzeniem budżetu na kolejne lata, aby umożliwić prawidłową alokację aktywów).

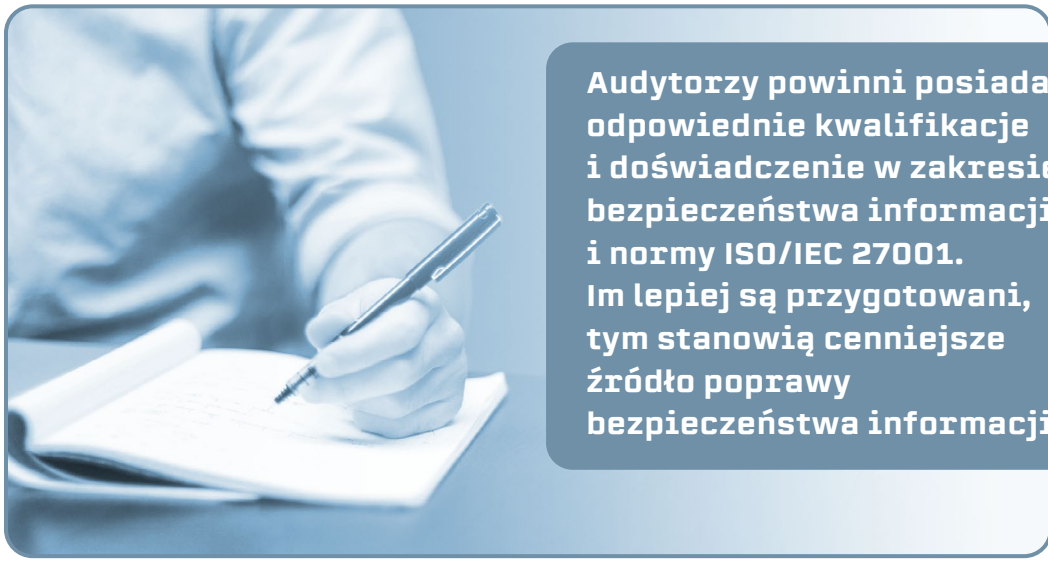
Plan powinien również zawierać wyniki nowych działań sugerowanych lub podyktowanych czynnościami wykonywanymi w ramach następnego *Kroku 4.3*.

Krok 4.3 Kontroluj bezpieczeństwo informacji

Skutecznym sposobem na sprawdzenie, czy bezpieczeństwo informacji utrzymywane jest na prawidłowym poziomie, jest planowanie i przeprowadzanie **audytów bezpieczeństwa informacji.** Takie audyty powinny odbywać się przynajmniej raz w roku.

Audytorzy powinni być wybierani spośród bezstronnych ekspertów w danej dziedzinie. Ich zadaniem powinno być weryfikowanie zgodności procesów bezpieczeństwa informacji z wymogami wewnętrznymi i zewnętrznymi.

Jeśli audyt przeprowadzany jest przez pracowników wewnętrznych, audytor nie może jednocześnie realizować zadań operacyjnych w zakresie zarządzania bezpieczeństwem informacji, tak aby uniknąć konfliktu interesów.



Audytorzy powinni posiadać odpowiednie kwalifikacje i doświadczenie w zakresie bezpieczeństwa informacji i normy ISO/IEC 27001. Im lepiej są przygotowani, tym stanowią cenniejsze źródło poprawy bezpieczeństwa informacji.

W wyniku przeprowadzonego audytu kadra kierownicza wyższego szczebla organizacji powinna otrzymać raport wyszczególniający:

- niezgodności, tj. aspekty, w których organizacja nie spełnia standardu;
- możliwości doskonalenia, tj. zalecenia wskazujące możliwość pracy w bezpieczniejszy sposób (mimo tego, że standard jest spełniony).

Niezgodności należy dokładnie przeanalizować i wdrożyć działania naprawcze, aby uniknąć ich ponownego pojawienia się w przyszłości.

Tego rodzaju działania muszą być zawarte w zaktualizowanej wersji Planu Bezpieczeństwa Informacji wraz z działaniami korygującymi niezgodności.

Możliwości doskonalenia powinny zostać ocenione i, jeśli to konieczne, ujęte również w ramach Planu Bezpieczeństwa Informacji. Mają one zazwyczaj niższy priorytet niż działania zmierzające do wyeliminowania niezgodności.

Krok 4.4 Monitoruj bezpieczeństwo informacji

Po zdefiniowaniu i zaprojektowaniu zabezpieczeń ujętych w poprzednim kroku, organizacja może powrócić do działania „w normalnym trybie". Aby zapewnić skuteczność systemu, należy wdrożyć działania monitorujące, które pomogą ograniczyć występowanie odchyleń od pierwotnego Planu Bezpieczeństwa Informacji.

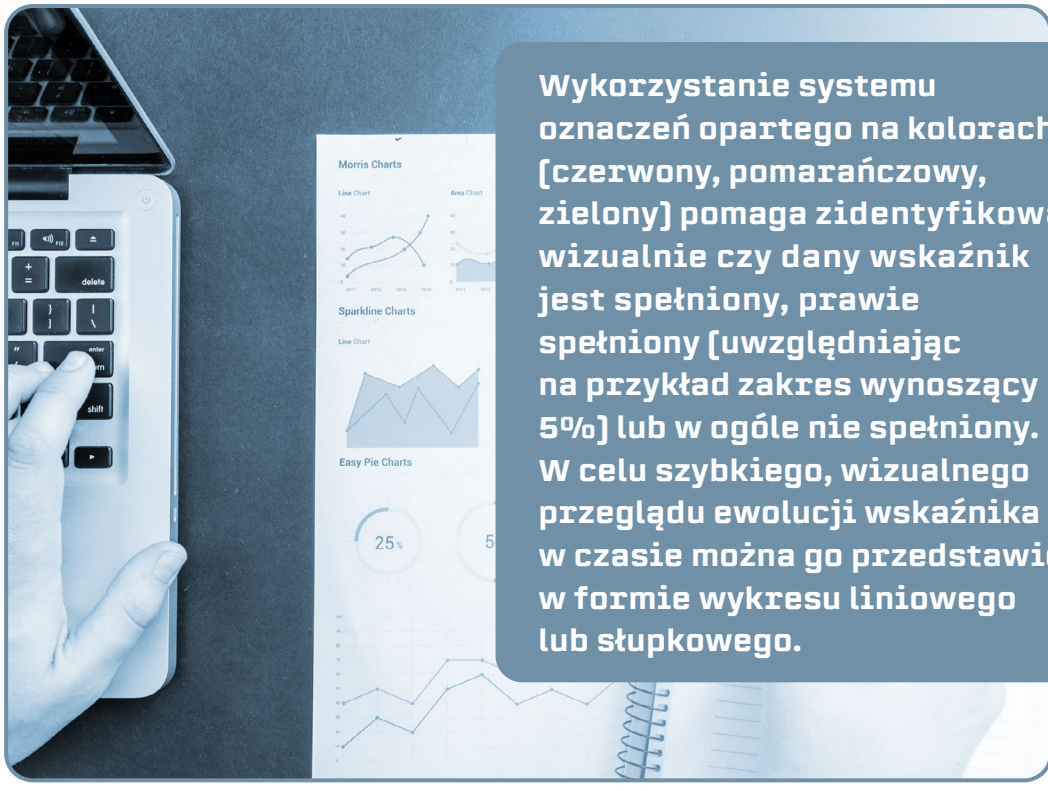
Najbardziej praktycznym sposobem prowadzenia działań monitorujących jest skonstruowanie prostych i praktycznych wskaźników określających cel lub skuteczność: Wskaźniki te mogą być okresowo aktualizowane.

Wskaźniki tego typu mogą opierać się na celach lub zabezpieczeniach. W gruncie rzeczy stanowią one wzory do obliczania progów, które w momencie ich naruszenia lub osiągnięcia, powinny informować o potrzebie podjęcia działań.

Ważne jest, aby przypisać odpowiedzialność za okresowe stosowanie wzoru do wskaźnika. Norma ISO/IEC 27004 może pomóc przy opracowywaniu tego zadania.

Wskaźniki dotyczące celu są najprostszymi wskaźnikami do skonfigurowania. Mogą być stosowane do pomiaru osiągnięcia istotnego celu dla organizacji, jakim jest uzyskanie zgodności z obowiązującymi wytycznymi lub z odpowiednim rozporządzeniem/ standardem czy wymaganym poziomem lub stanem usług związanych z bezpieczeństwem.

Wskaźniki powinny one być weryfikowane co kilka miesięcy.



Wykorzystanie systemu oznaczeń opartego na kolorach (czerwony, pomarańczowy, zielony) pomaga zidentyfikować wizualnie czy dany wskaźnik jest spełniony, prawie spełniony (uwzględniając na przykład zakres wynoszący 5%) lub w ogóle nie spełniony. W celu szybkiego, wizualnego przeglądu ewolucji wskaźnika w czasie można go przedstawić w formie wykresu liniowego lub słupkowego.

Wskaźniki skuteczności mogą być powiązane z niektórymi wartościami dotyczącymi efektywności osiaganych w procesach bezpieczeństwa informacji (np. oceny ryzyka) lub skuteczności zabezpieczeń. W tym ostatnim przypadku podstawowe zabezpieczenia zaproponowane w Kroku 3.1 można powiązać ze wskaźnikami, jak w przykładach poniżej:

Zabezpieczenie	Formuła wskaźnika	Cel	Cykliczność
Polityka bezpieczeństwa informacji	% pracowników, którzy otrzymali treść polityki	100%	raz w roku
Organizacja bezpieczeństwa informacji	# posiedzeń komitetu sterującego ds. bezpieczeństwa informacji	4	raz w roku
Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	% przeszkolonych pracowników, # inicjatyw mających na celu zwiększenie świadomości bezpieczeństwa	100%	raz w roku
Wykaz aktywów	% aktywów ujętych w wykazie w ciągu 1 miesiąca od dnia ich nabycia	100%	raz na kwartał
Ochrona przed przed złośliwym oprogramowaniem	# zainfekowanych stacji roboczych/ oczyszczonych stacji roboczych	1	raz w miesiącu
Aktualizacje usuwające podatności w oprogramowaniu	# zaległych krytycznych poprawek zabezpieczeń	0	raz w miesiącu
Bezpieczeństwo w umowach z dostawcami	% umów zawierających sprecyzowane klauzule dotyczące bezpieczeństwa informacji	100%	raz na kwartał
Analiza incydentów i reakcja na nie	# zamkniętych incydentów bezpieczeństwa informacji/otwartych incydentów bezpieczeństwa informacji w tym samym dniu	95%	raz w miesiącu

Tabela 7: Sugerowana cykliczność monitorowania zabezpieczeń

To tylko niektóre z podstawowych przykładów. Każda organizacja musi spójnie określić swoje własne wskaźniki. Wskaźniki te, monitorowane w prostym arkuszu, mogą być okresowo analizowane przez oficera/menadżera bezpieczeństwa informacji lub przedstawiane komitetowi sterującemu ds. bezpieczeństwa informacji.

Każdy z założonych celów powinien mieć ustalony termin realizacji.

Inne progi mogą zmieniać się w czasie i być początkowo ustalane poniżej docelowej wartości i rosnąć wraz z dojrzałością procesu lub zastosowanego zabezpieczenia.

Komitet sterujący ds. bezpieczeństwa informacji może okresowo monitorować stan i rozwój systemu zarządzania bezpieczeństwem informacji.

4 CERTYFIKACJA ISO/IEC 27001

Zaproponowane do tej pory podejście jest ściśle związane z wymaganiami normy ISO/IEC 27001, co pokazuje poniższa tabela.

Przypadki braku zgodności pomiędzy międzynarodowym standardem a tym poradnikiem są efektem uproszczonego podejścia przyjętego przez autorów tego poradnika. Celem takiego podejścia było zrezygnowanie z analizy kwestii formalnych i metodologicznych i skupienie się przede wszystkim na najbardziej praktycznych aspektach.

Główne rozdziały normy ISO/IEC 27001:2013		Kroki w poradniku dla MŚP z sektora ICT
4. Kontekst organizacji		
4.1	Zrozumienie organizacji i jej kontekstu	Krok 3
4.2	Zrozumienie potrzeb i oczekiwań stron zainteresowanych	Krok 2
4.3	Określenie zakresu systemu zarządzania bezpieczeństwem informacji	Nie dotyczy
4.4	System zarządzania bezpieczeństwem informacji	Nie dotyczy
5. Przywództwo		
5.1	Przywództwo i zaangażowanie	Nie dotyczy
5.2	Polityka	Zabezpieczenie podstawowe A1.01
5.3	Role, odpowiedzialność i uprawnienia	Krok 1
6. Planowanie		
6.1	Działania odnoszące się do ryzyk i szans	Krok 2 Krok 3
6.2	Cele bezpieczeństwa informacji i planowanie ich osiągnięcia	Nie dotyczy
7. Wsparcie		
7.1	Zasoby	Nie dotyczy
7.2	Kompetencje	Nie dotyczy
7.3	Uświadamianie	Zabezpieczenie podstawowe A1.03

7.4	Komunikacja	Zabezpieczenie dodatkowe A2.01
7.5	Udokumentowane informacje	Nie dotyczy
8. Działania operacyjne		
8.1	Planowanie i nadzór nad działaniami operacyjnymi	Krok 4
8.2	Szacowanie ryzyka w bezpieczeństwie informacji	Krok 2 Krok 3
8.3	Postępowanie z ryzykiem w bezpieczeństwie informacji	Krok 4
9. Ocena wyników		
9.1	Monitorowanie, pomiary, analiza i ocena	Krok 4
9.2	Audyt wewnętrzny	Krok 4
9.3	Przegląd zarządzania	
10. Doskonalenie		
10.1	Niezgodność i działania korygujące	Krok 4
10.2	Ciągłe doskonalenie	

Niemniej jednak należy zająć się każdym przypadkiem braku zgodności w momencie, gdy organizacja zdecyduje się uzyskać certyfikację według normy ISO/IEC 27001 jako kolejny krok, po zarządzaniu bezpieczeństwem informacji na podstawie zaleceń niniejszego poradnika. Mówiąc dokładniej, należy podjąć kolejne dodatkowe działania następujące po *Kroku 1.1*, jak przedstawiono w rozdziale 3.

Krok 1.2: Stwórz System Zarządzania Bezpieczeństwem Informacji (ISMS)

System Zarządzania Bezpieczeństwem Informacji (ang. ISMS) należy uznać za bardziej sformalizowane podejście do zarządzania bezpieczeństwem informacji niż podejście opisane w niniejszym poradniku.

ISMS obejmuje polityki, procedury, wytyczne oraz towarzyszące im aktywa i działania, którymi organizacja kolektywnie zarządza w celu ochrony swoich informacji. Kadra kierownicza wyższego szczebla powinna być bezpośrednio zaangażowana w planowanie ISMS, który wprowadza więcej wymogów formalnych, ale też zbliża organizację do zdobycia międzynarodowego certyfikatu dla którejś z jej części. Należy zachować dbałość przy wyborze właściwej części, ponieważ jego powiększenie bezpośrednio wpływa na koszty certyfikacji. Wybór całej organizacji jest możliwy, choć nie jedyny, ponieważ kluczowe usługi lub procesy mogą być traktowane priorytetowo zgodnie ze strategiami biznesowymi organizacji. Należy pamiętać, że jest również możliwe, aby certyfikować tylko jedną część ISMS.

Zaangażowanie kadry kierowniczej wyższego szczebla na wczesnym etapie jest niezbędne przy formułowaniu zakresu, jak również do pozyskania dodatkowego kluczowego zaangażowania (a co za tym idzie środków) do wykorzystania w następnych krokach. Postęp dotyczący implementacji powinien być regularnie raportowany, z uwzględnieniem terminów realizacji ustalonych dla tej implementacji.

W tej fazie należy przedstawić i wybrać cele mierzalne i okołobiznesowe.

Cele te, podobnie jak cała reszta ISMS, zawsze powinny się koncentrować na ciągłym doskonaleniu, iteracja po iteracji.

Pozostałe elementy

Podejście do zarządzania dokumentacją, którego należy przestrzegać w ramach formalnego ISMS (i każdego systemu zarządzania), nakłada wymóg, by każdy stworzony dokument:

- zawierał pełne metadane (przynajmniej tytuł, data, autor);
- opierał się na ustalonych formatach i modelach;
- podlegał kontroli zmian/wersji;
- trafiał do wyznaczonego odbiorcy.

Dokument stanowiący deklarację stosowania zgodnie z normą ISO/IEC 27001 wymóg 6.1.3 d) należy stworzyć i aktualizować na bieżąco.

Szablon wyboru zabezpieczenia proponowany w niniejszym poradniku stanowi dobry punkt wyjścia, przy czym jako minimum musi zawierać uzasadnienie włączenia lub wyłączenia każdego z zabezpieczeń.

Formalny przegląd zarządzania, który obejmuje wszystkie dane wejściowe określone w normie ISO/IEC 27001, wymóg 9.3, musi być również dokonywany okresowo. Powinien on korzystać z podejścia zaproponowanego w Kroku 3.2, ale należy go również w ramach tworzonej procedury opisać. Można go również rozszerzyć o formalną certyfikację dokonywaną przez niezależną jednostkę certyfikującą. Może być ona przeprowadzona w taki sam sposób jak audyt wewnętrzny, przy jednoczesnym wykorzystaniu zewnętrznego i kompetentnego spojrzenia na ISMS.

5 ODNIESIENIA DO DOKUMENTÓW ORAZ OGÓLNODOSTĘPNYCH ŹRÓDEŁ

ODNIESIENIA

- ISO/IEC 27000 family – Information security management systems.
  Tekst dostępny pod adresem: https://www.iso.org/isoiec-27001-information-security.html
- CEN Workshop Agreement (CWA) 16458 on European ICT Professional Profiles.
  Tekst dostępny pod adresem: ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA%2016458.pdf

OGÓLNODOSTĘPNE ŹRÓDŁA

- BSI. ISO/IEC 27001 for small and medium-sized businesses (SMEs).
  Tekst dostępny pod adresem: https://www.bsigroup.com/en-GB/iso-27001-information-security/ISO- 27001-for-SMEs/
- Centre for Cyber Security Belgium. Cyber Security Guide for SMEs.
  Tekst dostępny pod adresem: https://ccb.belgium.be/en/document/guide-sme
- European Union Agency For Network And Information Security (ENISA). *Information security and privacy standards for SMEs.* Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.
  Tekst dostępny pod adresem: https://www.enisa.europa.eu/publications/standardisation-for- smes/at_download/fullReport
- ENISA. *Security guide and online tool for SMEs when going Cloud.*
  Tekst dostępny pod adresem: https://www.enisa.europa.eu/news/enisa-news/enisa2019s-security-guide-and-online-tool-for-smes-when-going-cloud
- ENISA. *A simplified approach to Risk Management for SMEs.*
  Tekst dostępny pod adresem: https://www.enisa.europa.eu/publications/archive/RMForSMEs
- ETSI. *NIS Directive Implementation – ETSI TR 103 456 – technical report released by ETSI's technical committee on Cybersecurity (TC CYBER).*
  Tekst dostępny pod adresem: http://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_1034 56v010101p.pdf
- ISO. *Publicly available standards (including ISO/IEC 27000).*
  Tekst dostępny pod adresem: http://standards.iso.org/ittf/PubliclyAvailableStandards/

ANNEKS A

A.1 Zabezpieczenia podstawowe

L.p.	Nazwa zabezpieczenia	Numer w zał. A normy ISO/IEC 27001	Opis zabezpieczenia i zalecenia
01	**Polityka bezpieczeństwa informacji**	5.1.1 5.1.2	Należy uzgodnić politykę bezpieczeństwa informacji, a następnie ją opublikować i podać do wiadomości wszystkim pracownikom i odpowiednim osobom trzecim. Polityka powinna być poddawana przeglądom i weryfikowana w zaplanowanych odstępach czasu oraz w przypadku zaistnienia istotnych zmian, aby zapewnić jej adekwatność i skuteczność. *Sugerowana częstotliwość przeglądu: raz w roku*
02	**Organizacja bezpieczeństwa informacji**	6.1.1 6.1.2	Należy zdefiniować, przypisać i udokumentować role i zakres odpowiedzialności pracowników, kontrahentów i innych stron w zakresie bezpieczeństwa. Obowiązki i zakresy odpowiedzialności nie mogą się pokrywać, aby zminimalizować straty, jakie mogą zostać spowodowane niewłaściwym działaniem.
03	**Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji**	7.2.2	Należy regularnie szkolić wszystkich pracowników, kontrahentów i odpowiednie osoby trzecie oraz uświadamiać ich o zagrożeniach związanych z bezpieczeństwem informacji. Szkolenia powinny także obejmować politykę bezpieczeństwa informacji i procedury wdrożone przez organizację. *Sugerowana częstotliwość szkoleń: raz w roku*
04	**Wykaz aktywów**	8.1.1 8.1.2 8.1.3 8.1.4	Należy sporządzić i prowadzić scentralizowany wykaz ewidencji aktywów oraz go aktualizować. Należy zidentyfikować, udokumentować, zatwierdzić i wprowadzić własność i odpowiedzialność za wszystkie aktywa. Ponadto, należy sporządzić procedurę zarządzania wszystkimi aktywami przypisanymi pracownikom lub osobom trzecim, a następnie zapewnić identyfikowalność tychże aktywów przez cały okres ich użytkowania. *Sugerowana częstotliwość przeglądu: raz w miesiącu*
05	**Klasyfikacja, oznaczanie i przetwarzanie informacji**	8.2.1 8.2.2 8.2.3	Informacje należy klasyfikować, oznaczać i przetwarzać zgodnie z ich bezpośrednią wartością dla organizacji i obowiązującymi przepisami. Wszyscy właściciele informacji w organizacji powinni sporządzić i wdrożyć politykę oznaczania i przetwarzania informacji. *Sugerowane poziomy klasyfikacji informacji: publiczna, wewnętrzna, poufna*
06	**Identyfikacja użytkowników**	9.2.1 9.2.2	Każdemu użytkownikowi systemów i usług informatycznych powinien być przypisany unikalny identyfikator zgodnie z oficjalną procedurą rejestrowania i wyrejestrowywania, która pozwala przyznawać i odbierać użytkownikom dostęp.

L.p.	Nazwa zabezpieczenia	Numer w zał. A normy ISO/IEC 27001	Opis zabezpieczenia i zalecenia
07	**Autoryzacja użytkowników**	9.2.3 9.2.5 9.2.6	Przypisanie użytkownikom praw uprzywilejowanego dostępu do systemów i usług informatycznych należy monitorować i regularnie weryfikować, podobnie jak korzystanie z tych praw przez użytkowników. Użytkownicy powinni dysponować tylko minimalnymi prawami dostępu pozwalającymi im na wypełnianie swoich obowiązków. Każda zmiana w prawach dostępu powinna przebiegać zgodnie z procedurą, którą zatwierdza właściciel informacji.
08	**Uwierzytelnianie użytkowników**	9.2.4 9.3.1 9.4.1 9.4.2 9.4.3	Użytkownikom systemów i usług informacyjnych należy poufnie przypisać dane logowania, którymi będą mogli się uwierzytelnić. Zarówno same dane logowania, jak i sprawdzające je systemy informatyczne, powinny być odpowiednio zabezpieczone w celu minimalizacji ryzyka odgadnięcia przez osoby nieupoważnione. *Sugerowana siła danych logowania: 8 znaków nietworzących wyrazu ze słownika*
09	**Umiejscowienie aktywów**	11.2.1 11.2.2 11.2.3 11.2.6	Wszystkie aktywa zawierające dane oraz pomocnicze systemy informatyczne powinny znajdować się w miejscu zabezpieczonym przed przypadkowymi uszkodzeniami i zagrożeniami środowiskowymi oraz być podłączone do odpowiednich urządzeń peryferyjnych. Dotyczy to aktywów znajdujących się zarówno wewnątrz, jak i na zewnątrz siedziby organizacji.
10	**Ochrona przed przed złośliwym oprogramowaniem**	12.2.1	Wszystkie aktywa narażone na zainfekowanie złośliwym oprogramowaniem należy zabezpieczyć instalując i na bieżąco aktualizując oprogramowanie chroniące.
11	**Procedury bezpieczeństwa informacji**	12.1.1	Należy wdrożyć, udokumentować i utrzymywać procedury dotyczące bezpieczeństwa informacji oraz udostępniać je wszystkim użytkownikom.
12	**Aktualizacje usuwające podatności w oprogramowaniu**	12.5.1 12.6.1	Aktualizacje usuwające podatności, udostępniane przez dostawców oprogramowania, powinny być na bieżąco sprawdzane i instalowane na wszystkich urządzeniach. *Sugerowana częstotliwość instalowania aktualizacji: raz w miesiącu*
13	**Bezpieczeństwo sieci**	13.1.1 13.1.2	Sieci wykorzystujące ICT należy zaprojektować w taki sposób, aby zminimalizować ryzyko podsłuchiwania ruchu sieciowego i wprowadzania w nim niepożądanych zmian. Należy także ograniczyć komunikację pomiędzy zautoryzowanymi użytkownikami do niezbędnego minimum i blokować resztę komunikacji.
14	**Bezpieczeństwo w umowach z dostawcami**	15.1.1 15.1.2 15.1.3	Wszyscy dostawcy, z którymi organizacja wymienia informacje, powinni znać polityki bezpieczeństwa obowiązujące w organizacji, a umowy z nimi powinny nakazywać im przestrzegania tychże polityk, co pozwoli na przeprowadzanie weryfikacji. Te same zalecenia dotyczą podwykonawców pracujących z dostawcami.

15	**Analiza incydentów i reakcja na nie**	16.1.2 16.1.3 16.1.4 16.1.5	Wszyscy użytkownicy systemów i usług informatycznych powinni zgłaszać wszelkie zaobserwowane lub podejrzewane słabe punkty w zabezpieczeniach w celu analizy. Wyniki analizy pozwolą zastosować konkretne procedury reagowania na incydenty przy zachowaniu pełnego wglądu w sytuację w trakcie jej rozwoju.
16	**Identyfikacja wymagań prawnych i umownych**	18.1.1 18.1.4	Wszystkie mające zastosowanie wymagania dotyczące bezpieczeństwa informacji wynikające z krajowych, międzynarodowych i sektorowych przepisów należy na bieżąco monitorować, podobnie jak wymagania wynikające z umów zawartych z osobami trzecimi. Należy zwrócić szczególną uwagę na ochronę danych osobowych.

A.2 Zabezpieczenia dodatkowe

L.p.	Nazwa zabezpieczenia	Numer w zał. A normy ISO/IEC 27001	Opis zabezpieczenia i zalecenia
01	**Zarządzanie kontaktami zewnętrznymi i komunikacją**	6.1.3 6.1.4	Organizacja powinna nawiązać i utrzymywać stosowne kontakty z właściwymi organami władzy, aby umożliwić szybką reakcję na powszechne zagrożenia, oraz z grupami zainteresowanych specjalistów, forami i stowarzyszeniami z obszaru bezpieczeństwa, przede wszystkim w celu uzyskania rzetelnych informacji o zagrożeniach i zabezpieczeniach.
02	**Telepraca**	6.2.2	Należy wdrożyć politykę oraz wspierające ją zabezpieczenia w celu ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscu wykonywania telepracy. Narzędzia do telepracy należy opracowywać z uwzględnieniem dodatkowych zabezpieczeń, aby zapobiec wyciekowi i nadużywaniu informacji. System dostępu na odległość należy zabezpieczyć przed osobami nieupoważnionymi.
03	**Zarządzanie urządzeniami mobilnymi**	6.2.1	Należy odpowiednio skonfigurować zabezpieczenia w urządzeniach mobilnych wykorzystywanych do pracy, a także ściśle je monitorować.
04	**Postępowanie sprawdzające pracowników**	7.1.1	Należy sprawdzać przeszłość kryminalną oraz związane z nią informacje wszystkich pracowników i osób trzecich, którzy mają regularny dostęp do budynku organizacji, zgodnie z odpowiednimi przepisami prawa i zasadami etycznymi. Zakres takiej kontroli powinien być proporcjonalny do wymagań biznesowych.
05	**Klauzule w umowach pracowników**	7.1.2 7.2.3 7.3.1 13.2.4	Wszyscy pracownicy i osoby trzecie powinni podpisać umowę o zachowaniu poufności przed rozpoczęciem korzystania z danych organizacji. Umowa powinna też wymagać przestrzegania polityki bezpieczeństwa informacji stosowanej przez organizację oraz jasno przedstawiać konsekwencje jej nieprzestrzegania, w tym konsekwencje następujące po zmianie stanowiska bądź rozwiązaniu umowy.

L.p.	Nazwa zabezpieczenia	Numer w zał. A normy ISO/IEC 27001	Opis zabezpieczenia i zalecenia
06	**Zarządzanie nośnikami wymiennymi**	8.3.1 8.3.3 13.2.1 13.2.2 18.1.3	Obsługa wszelkich nośników wymiennych powinna być ograniczona konkretnymi zasadami. Nośniki zawierające informacje należy zabezpieczyć przed niepożądanym dostępem, nadużyciem i zniszczeniem w przypadku, gdyby znalazły się poza siedzibą organizacji.
07	**Usuwanie danych**	8.3.2 11.2.7	Należy stosować ścisłe procedury dotyczące bezpiecznego usuwania danych z nośników, które mają być wykorzystane do innych celów, bądź usunięte, w celu uniemożliwienia odzyskania poprzednich danych. *Sugerowany sposób usuwania danych: pełne nadpisanie*
08	**Polityka kontroli dostępu**	9.1.1 9.1.2	Należy udokumentować, prowadzić i dokonywać przeglądu oficjalnej polityki kontroli dostępu do systemu i sieci organizacji zgodnie z wymaganiami dotyczącymi bezpieczeństwa, klasyfikacji informacji i zarządzania nimi oraz poziomów uwierzytelniania pracowników.
09	**Szyfrowanie**	10.1.1 10.1.2	Należy opracować, udokumentować, wprowadzić, zachowywać oraz dokonywać okresowych przeglądów i aktualizować zabezpieczenia kryptograficzne wykorzystujące silne algorytmy, w celu zapewnienia poufności przechowywanych i przekazywanych informacji. Zaleca się stosowanie ścisłych, udokumentowanych procedur dotyczących użytkowania, zabezpieczania i przechowywania kluczy kryptograficznych przez cały okres ich użytkowania. *Sugerowane algorytmy szyfrujące: AES128+, SHA512+, RSA2048+*
10	**Bezpieczeństwo fizyczne**	11.1.1 11.1.2 11.1.3. 11.1.6	Należy zdefiniować bariery fizyczne i strefy bezpieczeństwa w celu zminimalizowania niepożądanego dostępu do budynku i systemów informatycznych organizacji oraz wyposażyć te bariery w system kontroli dostępu. Należy ograniczyć i odpowiednio zabezpieczyć punkty dostępu, w tym punkty ściągania i wysyłania danych.
11	**Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi**	11.1.4	Należy opracować i stosować w budynkach i znajdujących się w nich systemach informatycznych fizyczne zabezpieczenia przed katastrofami naturalnymi bądź innymi klęskami żywiołowymi czy też katastrofami spowodowanymi przez człowieka. *Sugerowane zagrożenia, które należy wziąć pod uwagę: pożar, wilgoć, trzęsienie ziemi*
12	**Konserwacja sprzętu**	11.2.4	Sprzęt należy konserwować zgodnie z Planem Bezpieczeństwa Informacji obowiązującym w organizacji. Należy monitorować dostęp do systemów informatycznych uzyskany w celach konserwacji.

13	**Stanowiska pracy i sprzęt bez nadzoru**	11.2.8 11.2.9	Przed pozostawieniem stanowiska pracy bez nadzoru, wszelkie urządzenia należy zawsze zabezpieczyć przed niepożądanym dostępem fizycznym i kradzieżą. Urządzenia należy zablokować po każdej sesji pracy oraz ustawić automatyczne wyłączanie po odpowiednim okresie nieaktywności. Na stanowiskach pracy nie należy zostawiać żadnych nośników danych bez nadzoru. *Sugerowany czas do automatycznego zamknięcia sesji lub włączenia wygaszacza ekranu: 15 minut*
14	**Zarządzanie zmianami**	12.1.2 12.6.2 14.2.2 14.2.4	Wszelkie zmiany w procesach i systemach organizacyjnych, biznesowych i informatycznych, które mogą wpłynąć na bezpieczeństwo informacji, należy rejestrować, zatwierdzać i sprawdzać. Zmiany w systemie i oprogramowaniu powinni wprowadzać wyłącznie upoważnieni pracownicy.
15	**Rozdział środowisk do opracowywania i testowania**	12.1.4 14.3.1	Należy w miarę możliwości rozdzielić infrastrukturę przeznaczoną do opracowywania i testowania oraz infrastrukturę operacyjną w celu zminimalizowania ryzyka nieupoważnionego dostępu do systemu operacyjnego. Ponadto, dane wykorzystywane do opracowywania i testowania powinny różnić się od danych wykorzystywanych do produkcji (tj. powinny być anonimowe lub niezwiązane z prawdziwymi osobami i zdarzeniami). *Sugerowany sposób rozdziału: odrębne systemy i sieci*
16	**Zapasowe kopie informacji**	12.3.1	Należy tworzyć i regularnie sprawdzać kopie zapasowe informacji i oprogramowania zgodnie z opracowaną polityką kopii zapasowych. *Sugerowana częstotliwość tworzenia kopii zapasowych: raz dziennie lub raz w tygodniu*
17	**Rejestracja i przechowywanie zdarzeń**	12.4.1 12.4.2 12.4.3	Należy rejestrować większość działań związanych z bezpieczeństwem, a rejestry należy zabezpieczać i chronić przed dostępem i zmianami oraz poddawać regularnemu przeglądowi. Wszelkie działania wykonywane przez administratorów i operatorów systemów powinny być rejestrowane jako udane bądź nieudane próby logowania i wylogowania. *Sugerowany okres przechowywania rejestrów: sześć miesięcy lub więcej*
18	**Synchronizacja zegarów**	12.4.4	Zegary systemowe we wszystkich działach organizacji lub domeny bezpieczeństwa należy na bieżąco synchronizować z jednym wzorcowym i rzetelnym źródłem czasu.
19	**Rozdzielenie sieci**	13.1.3	Usługi i systemy informatyczne oraz ich użytkowników należy rozdzielić w obrębie różnych obszarów sieci, przy czym we wszystkich obszarach powinny obowiązywać jednakowe wymagania dotyczące zabezpieczeń. Rozdziału należy dokonać za pomocą zapór ogniowych (ang. firewalls) lub podobnych rozwiązań.
20	**Bezpieczeństwo wiadomości i komunikacji elektronicznej**	13.2.3	Należy zapewnić poufność informacji przekazywanych za pomocą komunikatorów i podobnych systemów oraz wykrywać ataki dokonywane tą drogą.

L.p.	Nazwa zabezpieczenia	Numer w zał. A normy ISO/IEC 27001	Opis zabezpieczenia i zalecenia
21	**Uwzględnianie bezpieczeństwa na etapie projektowania rozwiązań**	6.1.4 14.1.1 14.2.5	Bezpieczeństwo informacji powinno być nieodłączną częścią systemów informatycznych przez cały okres użytkowania tychże systemów, w tym podczas wczesnej fazy projektowania. Wszelkie projekty podejmowane w organizacji powinny brać pod uwagę kwestie bezpieczeństwa informacji od jak najwcześniejszego etapu.
22	**Bezpieczeństwo usług aplikacyjnych**	14.1.2 14.1.3	Systemy informatyczne wykorzystywane do świadczenia usług powinny być chronione przed typowymi atakami za pomocą bezpiecznej, wzmocnionej konfiguracji. Powinny być także opracowywane w taki sposób, by mogły korzystać z dodatkowych zabezpieczeń i być na bieżąco monitorowane i chronione za pomocą dedykowanych środków bezpieczeństwa, proporcjonalnie do ich narażenia na ataki. *Sugerowane środki bezpieczeństwa: zapory ogniowe i IDS/IPS*
23	**Bezpieczny cykl opracowywania projektów**	14.2.1 14.2.6 14.2.7	Organizacja powinna ustanowić wytyczne dotyczące bezpiecznego cyklu opracowywania aplikacji, które można także będzie zastosować do projektów zewnętrznych wykonywanych na zlecenie w celu zminimalizowania podatności w aplikacjach.
24	**Testowanie bezpieczeństwa**	14.2.3 14.2.8 14.2.9 18.2.3	Należy ustanowić kryteria dotyczące bezpieczeństwa i zatwierdzania nowych systemów informatycznych oraz nowych aktualizacji i wersji oprogramowania. Ponadto każdy system należy odpowiednio testować w fazie opracowywania, przed zaakceptowaniem, a następnie w regularnych odstępach czasu. Wykryte podatności należy usunąć przed następnym testem. *Sugerowana częstotliwość testowania: testy wewnętrzne raz na sześć miesięcy, testy zewnętrzne raz na kwartał*
25	**Monitorowanie bezpieczeństwa usług świadczonych przez dostawców**	15.2.1 15.2.2	Należy regularnie monitorować, przeglądać i audytować dostarczanie usług zewnętrznych, w tym realne wypełnianie przez dostawców zapisów umownych.
26	**Polityka zarządzania incydentami**	16.1.1	Incydenty związane z bezpieczeństwem informacji należy kontrolować, rejestrować i przetwarzać oraz reagować na nie zgodnie z konkretnymi odpowiedzialnościami wprowadzonymi i zatwierdzonymi przez kierownictwo. Należy również wprowadzić odpowiednie procedury komunikacji i eskalacji.
27	**Wyciąganie wniosków z incydentów**	16.1.6	Wiedzę zdobytą podczas analizy i rozwiązywania incydentów związanych z bezpieczeństwem informacji należy wykorzystać do zredukowania prawdopodobieństwa wystąpienia lub skutku przyszłych incydentów. Może okazać się konieczne dostosowanie procedur reakcji na incydenty do nowych warunków.

28	**Zarządzanie redundancją**	17.2.1	Obiekty przetwarzające informacje należy wyposażyć w redundantne komponenty w taki sposób, by mogły spełnić wymagania dotyczące dostępności nawet podczas awarii.
29	**Ochrona własności intelektualnej**	18.1.2	Należy wdrożyć procedury zapewniające zgodność z wymaganiami prawnymi, regulacyjnymi i umownymi w zakresie wykorzystania materiałów objętych prawem własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.
30	**Audyty i oceny bezpieczeństwa informacji**	18.2.1 18.2.2	Niezależni audytorzy powinni regularnie dokonywać przeglądu systemów bezpieczeństwa informacji. Kierownictwo powinno zapewnić prawidłowe wdrażanie wszystkich procedur bezpieczeństwa w ramach swojego zakresu odpowiedzialności w celu uzyskania zgodności z politykami i normami bezpieczeństwa. Należy regularnie dokonywać przeglądu systemów informatycznych, aby zapewnić ciągłą zgodność z normami wdrażania bezpieczeństwa.

A.3 Związki pomiędzy zabezpieczeniami o charakterze dodatkowym a zagrożeniami (minimalizacja skutków)

Lp.	Zabezpieczenie	Ataki fizyczne	Nieumyślne szkody	Katastrofy	Awarie, usterki	Przerwy	Podsłuchiwanie, przechwycenie, porwanie	Naruszenie prawa	Nieetyczne działania, nadużycia
A2.01	**Zarządzanie kontaktami zewnętrznymi i komunikacją**	W*		P*		W	P		W
A2.02	**Telepraca**			W		W	P		
A2.03	**Zarządzanie urządzeniami mobilnymi**	W	W	W		W	P		W
A2.04	**Postępowanie sprawdzające pracowników**				W		P	P	W

*W – Wtórne, P– Pierwotne

Lp.	Zabezpieczenie	Ataki fizyczne	Nieumyślne szkody	Katastrofy	Awarie, usterki	Przerwy	Podsłuchiwanie, przechwycenie, porwanie	Naruszenie prawa	Nieetyczne działania, nadużycia
A2.05	Klauzule w umowach pracowników	W	W		W		P	P	P
A2.06	Zarządzanie nośnikami wymiennymi	P	P	W	W	W	P	W	
A2.07	Usuwanie danych	W	W		W		P		
A2.08	Polityka kontroli dostępu						P		P
A2.09	Szyfrowanie						P	P	
A2.10	Bezpieczeństwo fizyczne	P	W				P		
A2.11	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	P	W	P		P	W		
A2.12	Konserwacja sprzętu	P	P		P	W			
A2.13	Stanowiska pracy i sprzęt bez nadzoru	W					P		

A.2.14	Zarządzanie zmianami		W		W		P		W
A.2.15	Rozdział środowisk do opracowywania i testowania				W		W		
A.2.16	Zapasowe kopie informacji	P	P	P	P	W		W	W
A.2.17	Rejestracja i przechowywanie zdarzeń		W		W		P	W	P
A.2.18	Synchronizacja zegarów		W		W		P	W	P
A.2.19	Rozdzielenie sieci		W			W	P		W
A.2.20	Bezpieczeństwo wiadomości i komunikacji elektronicznej		W				P	W	W
A.2.21	Uwzględnianie bezpieczeństwa na etapie projektowania rozwiązań		W		W	W	P		P
A.2.22	Bezpieczeństwo usług aplikacyjnych		W				P	W	P
A.2.23	Bezpieczny cykl opracowywania projektów		P				P		W
A.2.24	Testowanie bezpieczeństwa		W				P		P

A.2.25	**Monitorowanie bezpieczeństwa usług świadczonych przez dostawców**				W	P		W	
A.2.26	**Polityka zarządzania incydentami**	W	W	W	W	W	W	W	W
A.2.27	**Wyciąganie wniosków z incydentów**	W	W	W	W	W	W	W	W
A.2.28	**Zarządzanie redundancją**			P	P	P		W	P
A.2.29	**Ochrona własności intelektualnej**							P	
A.2.30	**Audyty i oceny bezpieczeństwa informacji**		W				W	P	W

Załącznik X

Polityka bezpieczeństwa informacji		
Nr polityki:	**Data wejścia w życie:**	**Email:**
Wersja:	**Kontakt:**	**Tel.:**

Cel

Polityka bezpieczeństwa informacji i inne związane z nią polityki i procedury mają na celu ochronę poufności, integralności i dostępności wszystkich krytycznych danych i aktywów zgodnie z interesem organizacji.

Zakres

Polityka dotyczy pracowników, kontrahentów, konsultantów, pracowników tymczasowych i wszystkich innych pracowników organizacji, w tym pracowników zrzeszonych z osobami trzecimi. Polityka dotyczy również wszystkich aktywów, zarówno materialnych, jak i niematerialnych, należących do organizacji lub przez nią używanych.

Polityka

Kadra kierownicza wyższego szczebla organizacji uważa bezpieczeństwo informacji za jeden z kluczowych czynników wspierających jej działalność, w związku z czym angażuje się w promowanie i finansowanie wszystkich inicjatyw, które w wydajny i racjonalny pod względem kosztów sposób zmniejszają ryzyko związane z bezpieczeństwem informacji, zapewniają zgodność z odpowiednimi przepisami i wymogami kontraktowymi oraz są zgodne z sektorowymi zasadami dobrej praktyki. Od wszystkich wewnętrznych i zewnętrznych pracowników organizacji oczekuje się, że będą sumienne przestrzegać celu niniejszej polityki oraz wszystkich powiązanych z nią polityk i procedur oraz zawartych w nich zaleceń. Za nieprzestrzeganie tych zasad może być nałożona kara dyscyplinarna. W szczególności zasady bezpieczeństwa informacji, które wszyscy pracownicy powinny rozumieć i których powinni przestrzegać, są następujące:

1. bezpieczeństwo informacji nie jest pojęciem absolutnym, tzn. zabezpieczenia muszą być proporcjonalne do ryzyka;
2. przyznawanie dostępu musi ściśle wiązać się ze znajomością pracowników i ich potrzeb w pracy;
3. aktywa organizacji należy dzielić i chronić zgodnie z wymogami bezpieczeństwa informacji;
4. należy zawsze stosować otwarte standardy i rozwiązania zamiast rozwiązań zastrzeżonych i niejasnych;
5. pojedyncza warstwa zabezpieczeń chroniących informacje może nie wystarczyć w każdym przypadku, ponieważ zabezpieczenia mogą zawieść, dlatego w przypadkach, gdy konsekwencje przełamania zabezpieczeń byłyby wyjątkowo poważne, można stosować wiele warstw;
6. aby zapewnić szybką i skuteczną reakcję na zagrożenia, należy analizować sytuacje związane z bezpieczeństwem informacji oraz przeprowadzać odpowiednie testy;
7. bezpieczeństwo informacji jest odpowiedzialnością i obowiązkiem wszystkich osób w organizacji, a nie problemem kogoś innego.

Organizacja określa i wprowadza konkretne cele związane z bezpieczeństwem informacji. Cele te są na bieżąco monitorowane i dostosowywane i w zamierzeniu usprawniają podejmowanie decyzji taktycznych związanych z bezpieczeństwem informacji, podobnie jak wyżej wymienione zasady usprawniają podejmowanie decyzji strategicznych. Ciągłe doskonalenie jest kluczowym czynnikiem zapobiegającym stale rosnącym ryzykom związanym z bezpieczeństwem informacji i umożliwiającym organizacji osiąganie celów biznesowych we współczesnym, złożonym otoczeniu.

Zatwierdzanie i własność

Właściciel	Tytuł	Data	Podpis
Autor polityki	Tytuł	mm-dd-rrrr	
Zatwierdził(a)	**Tytuł**	**Data**	**Podpis**
Zespół kierowniczy	Tytuł	mm-dd-rrrr	

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki to wiodący pozarządowy ośrodek naukowo-badawczy o charakterze non-profit założony w 2000 r. Naszą misją jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski, jako aktywnego członka Unii Europejskiej oraz NATO. Instytut specjalizuje się w tworzeniu strategicznych rekomendacji i kierunków rozwoju kluczowych polityk publicznych, stanowiących merytoryczne wsparcie dla polskich i europejskich decydentów politycznych. Instytut Kościuszki jest pomysłodawcą i głównym organizatorem Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC, corocznej konferencji poświęconej strategicznym aspektom cyberprzestrzeni.

Publikacja współfinansowana przez Komisję Europejską i EFTA

sbs-sme.eu
@sbs-sme

digitalsme.eu
@eudigitalsme

Tłumaczenie i wydruk publikacji zostały sfinansowane w ramach projektu „Standaryzacja usług Hubów Innowacji Cyfrowej dla wsparcia cyfrowej transformacji przedsiębiorstw" współfinansowanego z Programu Ministra na lata 2019-2021 p.n. „Przemysł 4.0."