**Projekt zaliczeniowy z przedmiotu Standaryzacja Systemów Cyberbezpieczeństwa**

**Karol Ziobro cyberbezpieczeństwo, niestacjonarne**

Wstęp - opis firmy/organizacji

**Przygotowali:**

Karol Ziobro

Kamil Migacz

Piotr Grochot

Kamil Materowski

## Biuro księgowe. Lokalna siedziba, ma portal gdzie klient może zarządzać swoimi danymi. Może obsługiwać inne firmy

**POLITYKA BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW IT FIRMY *SKRYBA***

# Wstęp - opis firmy/organizacji

### Infrastruktura sieciowa i systemy

Firma posiada małe biuro wyposażone w karty do odbijania, które służą do kontroli dostępu. Sieć została podzielona na:

* Publiczną sieć Wi-Fi dla gości – dostęp po hasłach zmienianych okresowo.
* LAN dla pracowników – zabezpieczony firewallem i monitorowany.
* VPN – umożliwia księgowym pracę zdalną, z szyfrowaniem AES-256.

### Przechowywanie danych

* Storage na dane bieżącego roku podatkowego – z dwoma backupami (codziennymi i tygodniowymi).
* Główny serwer archiwizacyjny – przechowuje dane z ostatnich 10 lat, przenoszone automatycznie po zakończeniu roku podatkowego.
* Dwie bazy danych:
  + Baza danych bieżących – dostęp mają wszyscy księgowi.
  + Baza archiwalna – dostęp wyłącznie dla głównego administratora.

### Kontrola dostępu i uprawnienia

* Podział uprawnień – zaprojektowany tak, aby unikać konfliktów (np. edycja tylko przez wyznaczone osoby).
* Aplikacja do zabezpieczania faktur – wymaga uwierzytelnienia wieloskładnikowego (MFA).
* Użytkownicy (klienci) – mogą przeglądać swoje dane przez portal, ale edycja wymaga weryfikacji tożsamości (np. kodem SMS). Hasła zmieniane są co 90 dni.

### Zarządzanie danymi klientów

* Transfer danych – przy przejściu klienta do innej firmy dane są eksportowane w formacie PDF/XML z zabezpieczeniem hasłem.
* Dane po odejściu klienta – przechowywane przez 5 lat (zgodnie z wymogami prawnymi), a następnie usuwane z wykorzystaniem metod nadpisujących (np. DoD 5220.22-M).

### Polityka bezpieczeństwa

* Nadzór nad pracownikami – monitoring aktywności w systemie (logi dostępu, rejestracja operacji na plikach).
* Aktualizacje oprogramowania – automatyczne (critical updates) i comiesięczne (pozostałe poprawki).
* Narzędzia AI – dostęp do generatywnych modeli AI (np. ChatGPT) jest ograniczony do zadań niezwiązanych z danymi wrażliwymi.

### Zabezpieczenie komunikacji

* Poczta elektroniczna – szyfrowana (TLS), z filtrem antyspamowym.
* Polityka odpowiedzi – pracownicy odpowiadają tylko na maile zweryfikowanych klientów (z białej listy domen).

### Reagowanie na incydenty

* Wyciek danych – natychmiastowe odcięcie dostępu, powiadomienie UODO i klientów, analiza przyczyn.
* Procedura postępowania – obejmuje zmianę haseł, audyt logów i wdrożenie dodatkowych zabezpieczeń.

Wszystkie procesy są udokumentowane, a pracowncy regularnie szkoleni z zasad bezpieczeństwa.

1. Słownik 2

2. Cel i zakres opracowania 4

3. Klasyfikacja bezpieczeństwa zasobów IT 4

4. Bezpieczeństwo komunikacji sieciowej 5

5. Kontrola dostępu 6

6. Zabezpieczanie urządzeń końcowych 7

7. Urządzenia mobilne 8

8. Usługi chmurowe 9

9. Zarządzanie zmianą zasobów IT 9

10. Kopie zapasowe 10

11. Dostępność zasobów IT 10

12. Zarządzanie podatnościami zasobów IT 11

13. Eksploatacja i utrzymanie zasobów IT 11

14. Wycofywanie zasobów IT z eksploatacji 11

15. Bezpieczeństwo poczty elektronicznej 12

16. Bezpieczeństwo aplikacji webowych 12

17. Monitorowanie bezpieczeństwa IT 14

18. Bezpieczeństwo środowisk zwirtualizowanych 15

19. Bezpieczeństwo serwerów 16

20. Bezpieczeństwo IT 16

21. Edukacja i doskonalenie świadomości bezpieczeństwa IT 17

1. Infrastruktura sieciowa:

* Biuro: Małe biuro z kartami do odbijania.
* Zabezpieczenie sieci: Wdrożenie zabezpieczeń sieciowych (np. firewall, filtrowanie treści).
* Sieć:  
  + Sieć publiczna: Sieć dla gości z dostępem WiFi po haśle.
  + LAN: Sieć lokalna dla pracowników.
  + VPN: Możliwość pracy zdalnej za pomocą VPN.
  + System: Określenie systemu operacyjnego (np. Windows/Linux) oraz systemu kodowania (np. AES).

2. Serwery i Storage:

* Storage: Jeden serwer do przechowywania danych z roku podatkowego oraz dwa backupy na dane.
* Serwer archiwum: Jeden główny serwer archiwalny przechowujący dane do 10 lat wstecz.
* Standard przenoszenia danych: Określenie standardów i procedur przenoszenia danych z serwera do archiwum.

3. Uprawnienia i dostęp do danych:

* Bazy danych:  
  + Baza danych obecne: Dane bieżące.
  + Baza danych archiwum: Dane archiwalne.
* Dostęp:  
  + Tylko główny administrator ma dostęp do danych archiwalnych.
  + Zdefiniowanie uprawnień, by zapobiec konfliktom dostępu.

4. Zabezpieczenia i aplikacje:

* Zabezpieczenie faktur: Aplikacja, która może zabezpieczyć faktury przed nieautoryzowanym dostępem.
* Uwierzytelnianie klienta: Określenie sposobu uwierzytelniania klienta (np. login + hasło, 2FA).
* Zmiana haseł: Określenie częstotliwości zmiany haseł.
* Dostęp klienta do danych: Określenie, jakie dane klient może przeglądać i edytować.

5. Przenoszenie danych:

* Transfer danych: Standard przenoszenia danych klienta do innej firmy oraz z innej firmy.
* Usuwanie danych po odejściu klienta: Decyzja o tym, czy dane klienta powinny być usuwane, czy przechowywane po zakończeniu współpracy.

6. Polityki i procedury:

* Kontrola nad pracownikami: Polityka nadzorowania pracowników (np. monitorowanie działań na komputerze).
* Aktualizacja oprogramowania: Określenie częstotliwości aktualizacji oprogramowania na komputerach pracowników.
* Dostęp do narzędzi AI: Określenie możliwości dostępu pracowników do narzędzi AI w pracy.
* Zabezpieczenie maili: Polityka zabezpieczeń dla maili (np. szyfrowanie, filtry antywirusowe).
* Polityka komunikacji z klientami: Określenie, na jakie maile odpowiadać i jak reagować.
* Polityka wycieków danych: Określenie procedur w przypadku wycieku danych (co zrobić, jak reagować, kto informuje klientów).

**Rozdział 4. Bezpieczeństwo Komunikacji Sieciowej**

§ 4

1. **Właściciel/Kierownik Biura Rachunkowego** odpowiada za wdrożenie wymaganych mechanizmów zabezpieczeń kontroli ruchu sieciowego i transmisji danych w Biurze.
2. Przy planowaniu i wdrażaniu sieci komputerowej należy wziąć pod uwagę następujące aspekty:

2.1 **Wydzielenie sieci:** \* **Sieć dla pracowników (LAN i WiFi):** Zabezpieczona hasłem, przeznaczona do codziennej pracy księgowych. \* **Sieć dla gości (WiFi publiczne):** Oddzielna sieć bez dostępu do zasobów biura, służąca wyłącznie do przeglądania Internetu.

2.2 **Dostęp zdalny (VPN):** Pracownicy zdalni uzyskują bezpieczny dostęp do zasobów biura poprzez wirtualną sieć prywatną (VPN). Należy stosować silne metody uwierzytelniania dwuskładnikowego, jeśli to możliwe.

1. Wszelkie zmiany realizowane w środowisku sieci Biura i jego urządzeniach sieciowych wraz z Usługami IT wspierającymi właściwą eksploatację takiej sieci, podlegają akceptacji i dokumentacji przez Właściciela/Kierownika Biura.
2. Ruch w sieci jest kontrolowany za pomocą routera/firewalla w taki sposób, aby odrębne segmenty sieci (pracownicza, gościnna) były odseparowane od siebie logicznie.
3. Konfiguracja urządzeń sieciowych (router, przełączniki WiFi) nie powinna pozostawać w domyślnej konfiguracji producenta. Należy zmienić hasła dostępu do urządzeń, wyłączyć zbędne usługi i zabezpieczyć je zgodnie z najlepszymi praktykami.
4. W przypadku korzystania z zasobów IT spoza bezpośredniej kontroli Biura (np. chmura), muszą one spełniać wymagania bezpieczeństwa wynikające z poufności danych klientów.
5. Do zarządzania urządzeniami sieciowymi i serwerami wykorzystywane powinny być połączenia zapewniające szyfrowanie komunikacji (np. SSH, TLS, VPN).
6. Dostęp do zasobów IT powinien być ograniczony do czasu, w którym jest to niezbędne do wykonywania obowiązków.
7. Wysyłanie poufnych informacji poza sieć wewnętrzną (np. do klientów) wymaga stosowania mechanizmów szyfrowania (np. poprzez spakowanie plików chronionych hasłem, wykorzystanie bezpiecznych kanałów komunikacji).
8. Serwer przechowujący dane klientów powinien zapewniać mechanizmy szyfrowania przechowywanych danych (szyfrowanie dysku) oraz szyfrowanie transmisji danych przez sieć publiczną.

§ 4.1. Opis Sieci Biura Rachunkowego

Sieć biura rachunkowego będzie składać się z:

* **Sieci lokalnej (LAN):** Połączenie kablowe dla stacjonarnych komputerów w biurze.
* Sieci bezprzewodowej (WiFi):
  + **WiFi dla pracowników:** Zabezpieczone silnym hasłem (zgodnie z § 5 ust. 5), wykorzystujące standard szyfrowania WPA3 lub WPA2. Hasło powinno być regularnie zmieniane (np. co 3 miesiące).
  + **WiFi dla gości:** Oddzielna, publiczna sieć bez hasła lub z prostym hasłem udostępnianym na żądanie, z ograniczonym dostępem do Internetu i bez dostępu do zasobów wewnętrznych biura.
* **Wirtualnej Sieci Prywatnej (VPN):** Umożliwiającej bezpieczne połączenie zdalne dla księgowych pracujących poza biurem. Należy stosować silne protokoły VPN (np. OpenVPN, WireGuard) i silne metody uwierzytelniania.
* **System operacyjny serwera:** Zaleca się wykorzystanie serwerowego systemu operacyjnego (np. Linux Server, Windows Server) z regularnymi aktualizacjami zabezpieczeń.
* **Kodowanie danych:** Wszystkie wrażliwe dane przechowywane na serwerach powinny być szyfrowane. Zaleca się stosowanie silnych algorytmów szyfrowania (np. AES-256).

§ 4.2. Przechowywanie Danych i Archiwizacja

* **Bieżący rok podatkowy:** Dane za bieżący rok podatkowy będą przechowywane na dedykowanym storage'u.
* **Backupy:** Wykonywane będą co najmniej dwa backupy danych z bieżącego roku podatkowego. Backupy powinny być przechowywane w oddzielnych lokalizacjach (fizycznie i/lub w chmurze) i regularnie testowane pod kątem możliwości przywrócenia.
* **Archiwum:** Główny serwer będzie przeznaczony do archiwizacji danych (5 lat wstecz).
* **Standard przenoszenia danych do archiwum:** Po zakończeniu roku podatkowego i zamknięciu ksiąg, dane z bieżącego storage'u zostaną przeniesione na serwer archiwum. Proces ten powinien być udokumentowany. Dostęp do archiwum będzie ograniczony.
* Bazy danych:
  + **Baza danych "Dane Obecne":** Zawiera dane klientów za bieżący i potencjalnie poprzedni rok podatkowy.
  + **Baza danych "Dane Archiwum":** Zawiera dane klientów zarchiwizowanych (do 5 lat wstecz). Dostęp do tej bazy będzie miał tylko **Właściciel/Kierownik Biura**.

Rozdział 5. Kontrola Dostępu

§ 5

1. Zasady kontroli dostępu do zasobów IT muszą uwzględniać:

1.1. **Zasadę wiedzy koniecznej:** Każdy pracownik powinien mieć dostęp tylko do tych danych i systemów, które są mu niezbędne do wykonywania swoich obowiązków.

1.2. **Zasadę minimalnych uprawnień:** Pracownikom należy przydzielać tylko te uprawnienia, które są wymagane do realizacji ich zadań.

1.3. **Zasadę rozdziału uprawnień:** Uprawnienia księgowych powinny być rozdzielone w taki sposób, aby żaden pojedynczy pracownik nie miał pełnej kontroli nad wszystkimi aspektami przetwarzania danych (np. jeden księgowy nie powinien mieć możliwości wprowadzania i zatwierdzania płatności bez nadzoru).

\* **Księgowy:** Dostęp do danych klientów przypisanych do jego obsługi, możliwość wprowadzania i edytowania danych w zakresie swoich obowiązków.

\* **Właściciel/Kierownik Biura:** Pełny dostęp do wszystkich danych, możliwość zarządzania użytkownikami i uprawnieniami, dostęp do archiwum.

1.4. Wszystkie ograniczenia prawne dotyczące dostępu do danych osobowych i finansowych.

1. Autoryzacja (logowanie) musi się odbywać każdorazowo przed próbą uzyskania dostępu do systemów IT.
2. Dla każdego systemu IT (w tym serwera, baz danych) należy określić zakres i okres retencji logów (np. 3 miesiące). Logi powinny zawierać informacje o:

3.1. identyfikatorach użytkowników uzyskujących dostęp do informacji,

3.2. datach i czasach dostępu do informacji,

3.3. szczegółach działania (np. logowanie, edycja danych, eksport).

1. Zasady kontroli dostępu do systemów IT, w których przetwarzane są poufne informacje, muszą dodatkowo uwzględniać:

4.1. Ograniczenie liczby użytkowników z prawami administratora do minimum (najlepiej tylko Właściciel/Kierownik Biura).

4.2. Każdy system IT powinien posiadać co najmniej jedno konto awaryjne z wystarczającymi uprawnieniami do usunięcia awarii. Dane logowania do tego konta powinny być przechowywane w bezpiecznym miejscu i używane tylko w sytuacjach awaryjnych. Po użyciu hasło powinno zostać zmienione.

1. Zarządzanie uprawnieniami i kontrolą dostępu jest odpowiedzialnością Właściciela/Kierownika Biura.

5.1. Wszystkie systemy IT, tam gdzie jest to technicznie możliwe, muszą posiadać mechanizmy wymuszające silne hasła:

5.1.1. Hasła muszą mieć długość co najmniej 8 znaków.

5.1.2. Hasła muszą zawierać kombinację wielkich i małych liter, cyfr i znaków specjalnych.

5.1.3. Hasła nie mogą być łatwe do odgadnięcia ani być słownikowe.

5.1.4. Hasła nie mogą być przechowywane w postaci jawnej.

1. W przypadku trzech nieudanych prób logowania, konto użytkownika powinno zostać zablokowane na określony czas (np. 15 minut).
2. Konta użytkowników powinny być blokowane w przypadku:

7.1. Rozwiązania umowy o pracę.

7.2. Naruszenia zasad bezpieczeństwa.

§ 5.1. Aplikacja do Zabezpieczania Faktur

* Należy rozważyć wdrożenie dedykowanej aplikacji do zabezpieczania faktur, która oferuje funkcje szyfrowania, kontroli dostępu i śledzenia zmian.
* Dostęp do aplikacji powinien być zabezpieczony silnym hasłem i potencjalnie uwierzytelnianiem dwuskładnikowym.

§ 5.2. Uwierzytelnianie Klienta

* **Metody uwierzytelniania:** Klienci powinni być uwierzytelniani poprzez unikalny identyfikator (np. numer NIP) i hasło. Alternatywnie, można rozważyć bezpieczny portal klienta z logowaniem.
* **Częstość zmian hasła:** Zaleca się, aby hasła klientów były zmieniane co najmniej raz na 90 dni. System powinien wymuszać tworzenie silnych haseł.

§ 5.3. Wgląd i Edycja Danych przez Klienta

* **Możliwości wglądu:** Należy rozważyć udostępnienie klientom możliwości wglądu do ich danych poprzez bezpieczny portal online. Zakres wglądu powinien być jasno określony (np. podgląd faktur, sald).
* **Możliwości edycji:** Możliwość edycji danych przez klientów powinna być ograniczona do niezbędnego minimum i poddana weryfikacji (np. zmiana danych kontaktowych). Edycja danych księgowych powinna być możliwa tylko przez pracowników biura.

§ 5.4. Standard Przenoszenia Danych Klienta

* **Przenoszenie danych do innej firmy:** Na żądanie klienta, dane powinny być przekazane w powszechnie używanym i czytelnym formacie (np. pliki CSV, XML). Należy zapewnić bezpieczny sposób przekazania danych (np. zaszyfrowany e-mail, bezpieczny link do pobrania).
* **Przenoszenie danych z innej firmy:** Przy przejmowaniu obsługi klienta, należy ustalić z przyszłym biurem rachunkowym preferowany format przekazania danych. Należy zapewnić bezpieczny sposób odbioru danych.

§ 5.5. Usuwanie Danych po Odejściu Klienta

* **Polityka przechowywania:** Zgodnie z przepisami prawa, dane klientów powinny być przechowywane przez określony czas (np. 5 lat po zakończeniu roku podatkowego).
* **Usuwanie danych:** Po upływie wymaganego okresu przechowywania, dane klientów powinny zostać bezpiecznie usunięte (trwale usunięcie z systemów, fizyczne zniszczenie nośników). Należy prowadzić rejestr usuniętych danych.

Rozdział 6. Zabezpieczanie Urządzeń Końcowych

§ 6

1. Za zabezpieczanie urządzeń końcowych (komputerów, laptopów) odpowiada każdy pracownik biura. Właściciel/Kierownik Biura zapewnia niezbędne narzędzia i wsparcie.
2. Zabezpieczenia obejmują:

2.1 **Konfigurację urządzeń:** Zgodnie z zaleceniami producentów oprogramowania i standardami bezpieczeństwa.

2.2 **Implementację oprogramowania:** Instalacja i konfiguracja oprogramowania antywirusowego, zapory ogniowej (firewall), oprogramowania do szyfrowania dysku (w przypadku laptopów).

2.3 **Prowadzenie ewidencji:** Spis wszystkich urządzeń wykorzystywanych do pracy.

1. Konfiguracja urządzeń końcowych powinna obejmować:

3.1. Instalację tylko niezbędnego oprogramowania.

3.2. Regularną aktualizację zainstalowanego oprogramowania.

3.3. Wdrożenie zasad kontroli dostępu (silne hasła do logowania).

3.4. Wyłączenie zbędnych usług i procesów.

3.5. Zmianę domyślnych ustawień konfiguracyjnych.

1. Urządzenia końcowe powinny być skonfigurowane do automatycznej aktualizacji oprogramowania systemowego i zabezpieczającego.
2. Wszystkie urządzenia końcowe muszą posiadać zainstalowane i aktywne oprogramowanie antywirusowe z automatyczną aktualizacją baz sygnatur.
3. Oprogramowanie antywirusowe musi zapewniać ochronę w czasie rzeczywistym przed złośliwym oprogramowaniem.
4. W przypadku urządzeń niepodłączonych do Internetu, aktualizacje oprogramowania antywirusowego i systemowego muszą być przeprowadzane ręcznie, nie rzadziej niż raz w miesiącu. Odpowiedzialność za to ponosi użytkownik danego urządzenia.
5. Każdy przypadek wykrycia złośliwego oprogramowania musi być niezwłocznie zgłoszony Właścicielowi/Kierownikowi Biura.
6. Urządzenia końcowe powinny być chronione przed zagrożeniami (w tym złośliwym oprogramowaniem i spamem) poprzez odpowiednią konfigurację oprogramowania antywirusowego i potencjalnie dodatkowych narzędzi do ochrony.

Rozdział 7. Urządzenia Mobilne (Laptopy do Pracy Zdalnej)

§ 7

1. Właściciel/Kierownik Biura prowadzi ewidencję pracowników, którzy otrzymali laptopy do pracy zdalnej.
2. Laptopy pracowników zdalnych muszą być zabezpieczone zgodnie z zasadami określonymi dla urządzeń końcowych, ze szczególnym uwzględnieniem silnych haseł dostępu i szyfrowania dysku twardego.
3. Laptopy powinny mieć włączoną opcję automatycznego blokowania ekranu po określonym czasie bezczynności oraz ograniczenie liczby nieudanych prób logowania.
4. Procedura utylizacji laptopów lub dysków twardych, na których były przechowywane poufne dane, musi gwarantować trwałe i nieodwracalne usunięcie danych (np. fizyczne zniszczenie).
5. Naprawa laptopów zawierających poufne dane przez zewnętrznych dostawców IT może odbyć się dopiero po trwałym usunięciu wszystkich danych z dysku. W przypadku braku możliwości usunięcia danych, dysk twardy powinien zostać zniszczony.
6. Wsparcie techniczne w zakresie zabezpieczenia laptopów dla pracowników zdalnych zapewnia Właściciel/Kierownik Biura lub zewnętrzny dostawca IT.

§ 7.1. Polityka Dotycząca Kontroli/Nadzorowania Pracowników

* Nadzorowanie pracowników powinno odbywać się w sposób transparentny i zgodny z przepisami prawa.
* Możliwość monitorowania aktywności pracowników (np. logowanie do systemów) może być wykorzystywana w celu zapewnienia bezpieczeństwa i wykrywania potencjalnych nieprawidłowości. Pracownicy powinni być poinformowani o takiej możliwości.
* Nie dopuszcza się monitorowania treści prywatnych komunikacji pracowników.

§ 7.2. Częstotliwość Aktualizacji Oprogramowania Pracowników

* Oprogramowanie systemowe (system operacyjny) oraz oprogramowanie zabezpieczające (antywirus, firewall) na komputerach pracowników powinno być aktualizowane automatycznie, jeśli to możliwe.
* Pozostałe oprogramowanie wykorzystywane do pracy powinno być aktualizowane regularnie, zgodnie z zaleceniami producentów, nie rzadziej niż raz na kwartał. Właściciel/Kierownik Biura jest odpowiedzialny za monitorowanie dostępności aktualizacji i informowanie pracowników o konieczności ich instalacji.

§ 7.3. Dostęp do Narzędzi AI

* Dostęp do narzędzi AI (np. do analizy danych, wspomagania tworzenia dokumentów) powinien być rozważany indywidualnie, w zależności od potrzeb i potencjalnych zagrożeń bezpieczeństwa.
* Przed dopuszczeniem do korzystania z narzędzi AI należy ocenić ich politykę prywatności i bezpieczeństwa danych.
* W przypadku korzystania z narzędzi AI, które przetwarzają dane klientów, należy upewnić się, że dane te są odpowiednio zabezpieczone i przetwarzane zgodnie z obowiązującymi przepisami.

§ 7.4. Zabezpieczenia Maili

* Należy stosować silne hasła do kont pocztowych.
* Włączenie uwierzytelniania dwuskładnikowego dla kont pocztowych jest wysoce zalecane.
* Należy stosować filtry antyspamowe i antywirusowe na serwerze pocztowym.
* Pracownicy powinni być przeszkoleni w zakresie rozpoznawania phishingu i innych prób wyłudzenia informacji poprzez e-mail.

§ 7.5. Polityka dla Klientów – Na Jakie Maile Odpowiadać

* Należy jasno określić, jakie typy zapytań klientów są obsługiwane drogą mailową (np. prośby o informacje, przesłanie dokumentów).
* W przypadku bardziej złożonych spraw lub próśb wymagających weryfikacji tożsamości, zaleca się kontakt telefoniczny lub osobisty.
* Pracownicy powinni odpowiadać na maile klientów w sposób profesjonalny i z zachowaniem zasad poufności.

§ 7.6. Polityka Dotycząca Wycieków Danych – Sposób Zachowania

* W przypadku podejrzenia lub stwierdzenia wycieku danych, należy niezwłocznie poinformować Właściciela/Kierownika Biura.
* Należy wdrożyć procedurę reagowania na incydenty bezpieczeństwa, która określa kroki postępowania w przypadku wycieku danych (np. identyfikacja źródła wycieku, powiadomienie klientów i odpowiednich organów, podjęcie działań naprawczych).
* Każdy przypadek wycieku danych powinien być udokumentowany i analizowany w celu zapobieżenia podobnym incydentom w przyszłości.

§ 7.7. Karty do Odbijania

* Karty do odbijania służą do ewidencji czasu pracy pracowników w biurze oraz uzyskania przez nich dostępu do przestrzeni biurowej.
* Dane z kart do odbijania powinny być przechowywane w bezpieczny sposób i wykorzystywane wyłącznie do celów rozliczenia czasu pracy.
* Dostęp do danych z kart do odbijania powinien być ograniczony do upoważnionych osób (np. Właściciel/Kierownik Biura, dział kadr/płac).

Rozdział 8. Usługi chmurowe

§ 8

1. W biurze księgowym, przetwarzanie danych finansowych i osobowych w usługach chmurowych (publicznych lub prywatnych) może odbywać się tylko pod warunkiem, że przed rozpoczęciem korzystania z takich usług zostanie przeprowadzona ocena ryzyka, której celem jest określenie potencjalnych zagrożeń związanych z bezpieczeństwem tych danych. Ocena ryzyka powinna zostać wykonana przez Administratora Systemu Informatycznego (ASI) i uwzględniać specyfikę przetwarzania danych finansowych oraz wymogi ochrony danych osobowych zgodnie z RODO.

1. Usługi chmurowe wykorzystywane przez biuro księgowe muszą spełniać określone wymagania w zakresie bezpieczeństwa informacji, obejmujące:

2.1. Biuro księgowe powinno mieć możliwość zweryfikowania poziomu bezpieczeństwa infrastruktury, na której przechowywane i przetwarzane są dane. Powinno to obejmować certyfikaty bezpieczeństwa dostawcy usług oraz dostęp do dokumentacji związanej z bezpieczeństwem.

2.2. Usługi chmurowe muszą być wyposażone w systemy wykrywające i reagujące na potencjalne zagrożenia, takie jak nieautoryzowany dostęp, ataki hakerskie czy awarie systemowe. Mechanizmy te muszą umożliwiać szybką reakcję i minimalizację ryzyka utraty danych.

2.3. Wszystkie dane przetwarzane w chmurze, szczególnie dane finansowe i osobowe, muszą być szyfrowane zarówno w trakcie przechowywania (tzw. data at rest), jak i podczas przesyłania (data in transit). Szyfrowanie powinno wykorzystywać najnowsze i najbezpieczniejsze technologie.

2.4 Systemy chmurowe muszą umożliwiać precyzyjne określenie ról użytkowników oraz przypisanie im odpowiednich uprawnień do danych. Należy zapewnić, że każdy pracownik biura księgowego będzie miał dostęp tylko do tych informacji, które są niezbędne do realizacji jego obowiązków.

Rozdział 9. Zarządzanie zmianą zasobów IT

§ 9

1. Rozwój zasobów IT w biurze księgowym musi uwzględniać działania mające na celu wdrożenie właściwej ochrony systemów oraz informacji przetwarzanych z wykorzystaniem tych zasobów, a w szczególności:

1.1. Zasoby IT w biurze księgowym powinny mieć przypisaną odpowiednią klasyfikację informacji przetwarzanych, w szczególności danych osobowych, finansowych i wrażliwych klientów.

1.2. Każdy zasób IT, szczególnie w kontekście przetwarzania danych księgowych, musi być analizowany pod kątem wymagań bezpieczeństwa, zapewniając ochronę przed nieautoryzowanym dostępem i utratą danych.

1.3. Nowe zasoby IT, jak systemy księgowe, muszą być klasyfikowane pod kątem poziomu bezpieczeństwa, uwzględniając potencjalne ryzyko utraty danych finansowych i podatkowych.

1.4. W procesie projektowania nowych systemów IT (np. do zarządzania dokumentami i danymi klientów) należy uwzględnić bezpieczeństwo danych, takie jak szyfrowanie i kontrola dostępu.

1.5.Wszystkie systemy IT w biurze księgowym powinny przechodzić dokładne testy przed wdrożeniem, w celu weryfikacji zgodności z wymaganiami bezpieczeństwa, np. testy penetracyjne dla systemów finansowych.

1.6. W dokumentacji zasobów IT należy zawrzeć wszystkie zastosowane mechanizmy zabezpieczeń, takie jak szyfrowanie danych, zarządzanie dostępem i monitoring aktywności.

1. W procesie formułowania wymagań dla ochrony informacji i zasobów IT można stosować ogólnie dostępne standardy i najlepsze praktyki w zakresie bezpiecznego pisania kodu i realizacji funkcji, np. wytyczne NIST lub OWASP, dostosowane do wymagań biura księgowego.

1. Zasoby IT wykorzystywane do przetwarzania informacji chronionych, takich jak dane księgowe i osobowe klientów, muszą zapewniać mechanizmy bezpiecznej identyfikacji i weryfikacji tożsamości użytkowników. Domyślną metodą weryfikacji tożsamości powinno być stosowanie spersonalizowanych kont dostępowych i dwuskładnikowej autoryzacji.

1. Rozwój i testowanie systemów IT (np. oprogramowania księgowego lub CRM) musi odbywać się wyłącznie na danych testowych, które nie zawierają żadnych wrażliwych informacji dotyczących klientów lub transakcji.

1. Dokumentacja powykonawcza musi zawierać szczegółowe opisy wszystkich zastosowanych mechanizmów bezpieczeństwa IT w wdrożonych zasobach, takich jak konfiguracja zapór sieciowych, metody szyfrowania oraz procedury ochrony danych osobowych.

1. Zarządzanie zmianą zasobów IT wymaga zatwierdzenia przez Dyrektora IT biura księgowego, który odpowiada za zgodność z polityką bezpieczeństwa i normami dotyczącymi ochrony danych.

Rozdział 10. Kopie zapasowe

§ 10

1. Czynności realizacji tworzenia kopii zapasowych w biurze księgowym powinny uwzględniać następujące aspekty:

1.1. Tworzone kopie zapasowe muszą być w pełni zgodne z danymi przechowywanymi w systemach IT, w tym z danymi finansowymi, osobowymi i podatkowymi, które są podstawą działalności biura.

1.2. Każda kopia zapasowa powinna być jednoznacznie identyfikowana, aby zapobiec pomyłkom przy przywracaniu danych. Należy wykorzystywać oznaczenia nośników, takie jak unikalne identyfikatory.

1.3. Kopie zapasowe muszą umożliwiać pełne przywrócenie danych, w tym dokumentów księgowych, danych transakcyjnych i innych informacji wrażliwych, z zachowaniem integralności i bezpieczeństwa.

1. Zakres wymagań dotyczących tworzenia kopii zapasowych dla zasobów IT w biurze księgowym powinien obejmować:

2.1. Ile wersji kopii zapasowych powinno być przechowywanych w celu zapewnienia odpowiedniej ochrony przed utratą danych (np. ostatnie 30 wersji dokumentów księgowych).

2.2. Systemy IT muszą być dostępne w możliwie najkrótszym czasie po awarii. Czas przywrócenia (RTO) zależy od krytyczności danych, np. systemy księgowe muszą być przywrócone w ciągu kilku godzin.

2.3. Kopie zapasowe powinny być tworzone regularnie, np. codziennie dla aktywnych danych księgowych, a raz w tygodniu dla danych archiwalnych.

2.4. Kopie zapasowe powinny być przechowywane przez określony czas zgodnie z przepisami prawa dotyczącymi przechowywania danych księgowych.

1. Podczas tworzenia kopii zapasowych należy przestrzegać poniższych zasad, które obejmują co najmniej następujące informacje:

3.1. Należy rejestrować daty i godziny wykonania kopii zapasowych, aby zapewnić pełną historię działań.

3.2. Należy oznaczać kopie zapasowe według typu (np. kopia pełna, przyrostowa), aby ułatwić proces przywracania danych.

3.3. Należy rejestrować, które dane zostały objęte kopią zapasową (np. dane księgowe, pliki z deklaracjami podatkowymi).

3.4. Należy dokumentować miejsce przechowywania kopii zapasowych (np. chmura, nośnik fizyczny), aby w razie potrzeby móc szybko odnaleźć dane.

1. Dokumentacja, o której mowa w ust. 3, może być prowadzona w formie papierowej lub w przeznaczonym do tego celu zasobie IT, np. w systemie zarządzania kopiami zapasowymi, który zapewnia łatwy dostęp do informacji.

1. Zasady tworzenia kopii zapasowych dla każdego zasobu IT w biurze księgowym powinny być przygotowane przez odpowiedzialnego ASI aby zapewnić zgodność z wewnętrznymi politykami bezpieczeństwa danych.

Rozdział 11. Dostępność zasobów IT

§ 11

1. Zapewnienie dostępności zasobów IT obejmuje szereg działań, które mają na celu utrzymanie ciągłości działania systemów oraz ochronę danych przetwarzanych przez te zasoby. Do głównych celów takich działań należy:

1.1. Przeprowadzenie działań w trakcie rozwoju zasobu IT w celu ustalenia wymagań dotyczących dostępności oraz wdrożenia odpowiednich rozwiązań organizacyjnych i technicznych, które zapewnią ich spełnienie po wdrożeniu zasobu.

1.2. Działania organizacyjne lub techniczne mające na celu zapobieganie awariom oraz innym zdarzeniom, które mogą prowadzić do ograniczenia dostępności przetwarzanych informacji.

1.3. Działania organizacyjne lub techniczne, mające na celu minimalizowanie skutków awarii oraz innych zdarzeń, które mogą prowadzić do ograniczenia dostępności informacji, oraz zapewnienie ich przywrócenia w ustalonym czasie.

1.4. ASI ustala następujące parametry:

1.4.1. **RTO (Recovery Time Objective)** – maksymalny czas, jaki upływa od momentu wystąpienia sytuacji powodującej niedostępność informacji, do momentu przywrócenia dostępu do tych informacji.

1.4.2. **RPO (Recovery Point Objective)** – maksymalny dopuszczalny czas, przez który informacje mogą być niedostępne, nie powodując negatywnych skutków dla wspieranego przez zasób procesu.

Rozdział 12. Zarządzanie podatnościami zasobów IT

§ 12

1. Zasoby IT muszą być regularnie monitorowane i analizowane pod kątem występowania potencjalnych podatności (czyli słabości w systemach, które mogą zostać wykorzystane przez atakujących).

1. W zależności od klasyfikacji bezpieczeństwa zasobów IT, ich monitorowanie i badanie podatności może być bardziej lub mniej intensywne. Zasoby, które przetwarzają bardziej wrażliwe informacje lub są krytyczne dla funkcjonowania organizacji, powinny być monitorowane częściej i z większą dokładnością, aby jak najszybciej wykryć ewentualne luki w zabezpieczeniach.

1. Po zidentyfikowaniu podatności, konieczne jest przeprowadzenie odpowiednich działań naprawczych. Przed wdrożeniem jakichkolwiek zmian mających na celu eliminację podatności, należy je najpierw przetestować, aby upewnić się, że proponowane rozwiązanie jest skuteczne i nie wpłynie negatywnie na funkcjonowanie zasobu IT.

**Rozdział 13. Eksploatacja i utrzymanie zasobów IT**

§ 13.1. Regularne monitorowanie zasobów

1. **Zakres monitorowania**:
   * **Serwer główny i storage**:
     + Ciągłe śledzenie wykorzystania CPU, RAM, przestrzeni dyskowej (np. narzędzie **Zabbix**).
     + Alerty przy wykorzystaniu dysku >80% lub temperaturze serwera >70°C.
   * **Portal klienta**:
     + Monitorowanie dostępności (uptime) co 1 minutę (np. **UptimeRobot**).
     + Rejestracja wszystkich prób logowania (w tym adresów IP).
   * **Sieć LAN/WiFi**:
     + Wykrywanie nieautoryzowanych urządzeń (np. **ARPWatch**).
     + Analiza ruchu pod kątem ataków DDoS lub skanowania portów.
2. **Aktualizacje komponentów**:
   * Automatyczne aktualizacje systemów operacyjnych i oprogramowania w **oknach serwisowych** (np. w niedziele 02:00–04:00).
   * Krytyczne łaty (np. dla VPN lub firewalla) wdrażane są w ciągu **24 godzin** od publikacji.
   * Wyjątek: Aktualizacje portalu klienta wymagają **testów na środowisku stagingowym** przed wdrożeniem.
3. **Raportowanie**:
   * Codzienny raport dla ASI z podsumowaniem incydentów.
   * Miesięczne zestawienie dla Dyrektora Biura z metrykami bezpieczeństwa (np. liczba wykrytych zagrożeń).

§ 13.2. Przeglądy konfiguracji

1. **Harmonogram audytów**:
   * **Co 3 miesiące**: Weryfikacja konfiguracji firewalla (reguły dostępu, blokada portów).
   * **Co 6 miesięcy**:
     + Przegląd polityk szyfrowania (TLS, algorytmy kluczy).
     + Audyt uprawnień do baz danych (kto ma dostęp do danych klientów).
   * **Raz w roku**: Pełny audyt zgodności z RODO i Ustawą o rachunkowości.
2. **Narzędzia wspierające**:
   * **OpenVAS** do skanowania podatności w sieci wewnętrznej.
   * **Lynis** do audytu bezpieczeństwa serwerów.
3. **Korekty konfiguracji**:
   * Wszelkie zmiany wymagają **testów na środowisku izolowanym**.
   * Konfiguracje backupów muszą zapewniać **regułę 3-2-1** (3 kopie, 2 nośniki, 1 offsite).

§ 13.3. Serwisowanie przez dostawców IT

1. **Zasady ogólne**:
   * Dostawcy zewnętrzni podpisują **umowę NDA** oraz **klauzulę RODO**.
   * Lista zatwierdzonych dostawców jest aktualizowana co rok przez Dyrektora Biura.
2. **Serwis fizyczny (np. naprawa serwera)**:
   * Wymagane **protokoły czystości**:
     + Przed serwisem: Usunięcie danych z nośników za pomocą **DBAN** (Dwukrotne nadpisanie).
     + Po serwisie: Weryfikacja braku pozostawionych danych testowych.
   * Nadzór ASI jest obowiązkowy, chyba że Dyrektor zatwierdzi wyjątek.
3. **Serwis zdalny**:
   * Połączenia odbywają się przez **VPN z uwierzytelnianiem certyfikatem + 2FA**.
   * Sesje zdalne są nagrywane i przechowywane przez **30 dni**.
4. **Incydenty podczas serwisu**:
   * Wykrycie próby nieautoryzowanego dostępu = natychmiastowe przerwanie sesji.
   * Incydenty zgłaszane są do Dyrektora w ciągu **1 godziny**.

§ 13.4. Zarządzanie hasłami i dostępami

1. **Konta serwisowe**:
   * Hasła do kont dostawców IT zmieniane są po każdej wizycie serwisowej.
   * Dostęp ograniczony do konkretnych zasobów (np. tylko do serwera backupowego).
2. **Dostęp pracowników**:
   * Księgowi pracujący zdalnie łączą się przez **OpenVPN z certyfikatami TLS**.
   * Brak dostępu do danych archiwalnych (starszych niż 3 lata) dla pracowników zdalnych.

§ 13.5. Dokumentacja i szkolenia

1. **Rejestry**:
   * **Rejestr zmian konfiguracji**: Data, opis zmiany, osoba odpowiedzialna.
   * **Rejestr serwisów**: Data, zakres prac, nazwa dostawcy.
2. **Szkolenia**:
   * Co 6 miesięcy szkolenie pracowników z zasad bezpiecznego korzystania z systemów IT.

Rozdział 14. Wycofywanie zasobów IT z eksploatacji

§ 14.1. Zasady ogólne

1. **Definicja wycofania**:
   * Zasób IT uznaje się za wycofany z eksploatacji, gdy:
     + Nie jest używany dłużej niż **6 miesięcy**.
     + Został zastąpiony nowym systemem (np. migracja do chmury).
     + Jego utrzymanie stwarza ryzyko naruszenia bezpieczeństwa (np. brak wsparcia producenta).
2. **Plan wycofania**:
   * Każde wycofanie wymaga **planu technicznego** zatwierdzonego przez Dyrektora Biura, uwzględniającego:
     + Harmonogram działań (w tym archiwizację i usuwanie danych).
     + Listę osób odpowiedzialnych (ASI, księgowy nadzorujący dane).
     + Analizę ryzyka dla ciągłości działania.

§ 14.2. Bezpieczeństwo danych podczas wycofania

1. **Archiwizacja**:
   * Dane klientów z wycofywanego zasobu (np. serwer) są przenoszone do **zaszyfrowanego archiwum** na głównym serwerze (AES-256).
   * Przed przeniesieniem dane są weryfikowane pod kątem integralności (np. narzędzie **SHA-256** do generowania sum kontrolnych).
2. **Usuwanie danych**:
   * Wszystkie nośniki (dyski, taśmy backupowe) podlegają:
     + **Nadpisaniu** zgodnie z normą **NIST SP 800-88** (3-krotne nadpisanie losowymi danymi).
     + **Fizycznemu zniszczeniu**, jeśli nośnik nie nadaje się do ponownego użycia (np. niszczenie dysków przez strzępiarkę).
   * Wyjątek: Nośniki z danymi archiwalnymi (starszymi niż 10 lat) mogą być przekazane do **certyfikowanego centrum recyklingu** po zatwierdzeniu przez Dyrektora.
3. **Kwarantanna danych**:
   * Dane usunięte z systemu są przechowywane w **zaszyfrowanej "kwarantannie"** przez **30 dni** w celu umożliwienia odzyskania w przypadku błędu.

§ 14.3. Przenoszenie danych klienta

1. **Eksport do innej firmy**:
   * Dane klienta (np. faktury, ewidencje) są udostępniane w formacie **.zip zaszyfrowanym hasłem** (min. 12 znaków).
   * Hasło przesyłane jest **osobnym kanałem** (np. SMS, komunikator szyfrowany).
   * Klient otrzymuje **potwierdzenie wykonania eksportu** podpisane cyfrowo przez ASI.
2. **Import danych od klienta**:
   * Pliki importowane są analizowane pod kątem malware (np. **VirusTotal**).
   * Dane przechodzą **walidację strukturalną** (np. zgodność z formatem JPK).

§ 14.4. Niszczenie nośników

1. **Procedura niszczenia**:
   * **Dyski HDD/SSD**: Mechaniczne zniszczenie (np. niszczarka do dysków **SEM Shredder**) + potwierdzenie wykonania przez firmę zewnętrzną.
   * **Nośniki USB/Taśmy**: Stopienie w wysokiej temperaturze (np. współpraca z firmą **EcoTech Recycling**).
   * **Drukarki wielofunkcyjne**: Usunięcie i zniszczenie pamięci wewnętrznej.
2. **Dokumentacja**:
   * Każde niszczenie jest rejestrowane w **Rejestrze Zniszczeń** z podpisem ASI i Dyrektora.

§ 14.5. Dane po odejściu klienta

1. **Retencja danych**:
   * Dane klientów są przechowywane przez **5 lat** od końca współpracy (wymóg Ustawy o rachunkowości).
   * Po tym okresie podlegają anonimizacji (usunięcie NIP, nazwisk) i przeniesieniu do archiwum "tylko do odczytu".
2. **Żądanie usunięcia danych**:
   * Na wniosek klienta (np. zgodnie z RODO), dane są usuwane w ciągu **14 dni**, z wyjątkiem danych wymaganych prawem (np. dokumentacja podatkowa).

§ 14.6. Nadzór i kontrola

1. **Audyty**:
   * Co 6 miesięcy przeprowadzany jest **audyt procesu wycofywania** przez niezależnego konsultanta IT.
   * Sprawdzane są m.in.:
     + Kompletność dokumentacji.
     + Skuteczność usuwania danych (testy losowych nośników).
2. **Kary za naruszenia**:
   * Przekazanie danych bez nadpisania = zawieszenie uprawnień ASI.
   * Niezatwierdzone niszczenie nośników = odpowiedzialność finansowa pracownika.

§ 14.7. Procedura awaryjna

1. **Wykrycie danych na wycofanym nośniku**:
   * Natychmiastowe odzyskanie nośnika i powiadomienie Dyrektora.
   * Incydent zgłaszany do GIODO w ciągu **72 godzin**.
2. **Wyciek danych**:
   * Automatyczne zablokowanie kont klientów związanych z wyciekiem.
   * Wdrożenie procedury **PRG (Plan Reagowania na Incydenty)**.

Rozdział 15. Bezpieczeństwo poczty elektronicznej

1. **Zasady ogólne**:
   * Wszystkie maile z danymi klientów (np. faktury) muszą być szyfrowane protokołem **TLS 1.3**.
   * Zakaz przesyłania loginów/haseł do portalu klienta drogą mailową – wykorzystywany jest mechanizm „reset hasła” z weryfikacją SMS.
2. **Polityka dla pracowników**:
   * Pracownicy zdalni łączą się z firmową skrzynką wyłącznie przez **VPN z uwierzytelnianiem certyfikatami**.
   * Automatyczne skanowanie załączników pod kątem malware (np. narzędzie **ClamAV**).
3. **Komunikacja z klientami**:
   * Odpowiedzi na maile klientów tylko z domeny firmowej (@biuro-ksiegowe.pl).
   * Wiadomości z zewnętrznych domen zawierające podejrzane załączniki są blokowane.

Rozdział 16. Bezpieczeństwo aplikacji webowych

§ 16.1. Uwierzytelnianie i kontrola dostępu

1. **Wymagania dotyczące haseł**:
   * **Silne hasła**: Minimalna długość 12 znaków, wymagane użycie wielkich liter, cyfr i znaków specjalnych.
   * **Hasing haseł**: Hasła przechowywane z użyciem algorytmu **bcrypt** z solą (koszt minimum 12).
   * **Zmiana haseł**: Wymuszana co **90 dni** dla klientów i co **60 dni** dla pracowników.
   * **Historia haseł**: Blokada ponownego użycia 5 ostatnich haseł.
2. **Uwierzytelnianie dwuskładnikowe (2FA)**:
   * Obowiązkowe dla wszystkich kont z dostępem do danych klientów (np. **Google Authenticator** lub **SMS**).
   * Awaryjne kody jednorazowe przechowywane w zaszyfrowanej bazie danych.
3. **Blokada konta**:
   * Automatyczna blokada po **5 nieudanych próbach logowania**. Odblokowanie wymaga kontaktu z ASI.
   * Monitorowanie adresów IP podejrzanych o ataki brute-force (np. narzędzie **Fail2Ban**).

§ 16.2. Zarządzanie sesjami

1. **Generowanie tokenów sesji**:
   * Tokeny generowane z użyciem kryptograficznego generatora liczb losowych (**CSPRNG**).
   * Długość tokenu: **min. 128 bitów**.
2. **Bezpieczeństwo cookies**:
   * Atrybuty: **Secure**, **HttpOnly**, **SameSite=Strict**.
   * Prefiks **\_\_Host-** dla cookies związanych z domeną główną.
3. **Czas trwania sesji**:
   * Sesje wygasają po **15 minutach** bezczynności lub **4 godzinach** aktywności.
   * Mechanizm **automatycznego wylogowania** z powiadomieniem użytkownika.
4. **Ochrona przed sesją równoległą**:
   * Blokada wielosesyjności – tylko **jedno aktywne logowanie** na użytkownika.
   * Powiadomienia o nowym logowaniu (adres IP, data, urządzenie).

§ 16.3. Szyfrowanie i bezpieczeństwo transmisji

1. **Protokoły komunikacyjne**:
   * Wymuszony **TLS 1.3** na wszystkich podstronach i API.
   * Wyłączone przestarzałe protokoły (SSLv3, TLS 1.0/1.1).
2. **Konfiguracja certyfikatów**:
   * Certyfikaty SSL od zaufanych CA (np. Let's Encrypt, DigiCert).
   * Wdrożenie **HSTS** z maksymalnym czasem życia (max-age=63072000).
   * **Certificate Pinning** dla aplikacji mobilnych.
3. **Ochrona przed mixed content**:
   * Wszystkie zasoby (CSS, JS, obrazy) ładowane wyłącznie przez HTTPS.
   * Automatyczne przekierowanie HTTP → HTTPS z kodem **301**.

§ 16.4. Bezpieczeństwo kodu i danych

1. **Walidacja i sanitacja danych**:
   * Ochrona przed SQL Injection: wyłącznie **prepared statements** (np. ORM Hibernate).
   * Ochrona przed XSS: kodowanie wyjścia (np. **OWASP Java Encoder**).
2. **API**:
   * Autoryzacja przez **OAuth 2.0** lub **JWT** z krótkim czasem ważności tokenów (max 1 godzina).
   * Rate limiting: **100 żądań na minutę** na użytkownika.
3. **Maskowanie danych**:
   * Wrażliwe dane (np. NIP, PESEL) maskowane w interfejsie (np. \***123**).
   * Pełne dane widoczne tylko po dodatkowej autoryzacji (np. 2FA).

§ 16.5. Nagłówki bezpieczeństwa

1. **Content Security Policy (CSP)**:
   * Restrykcyjna polityka z wyłączeniem inline scripts i eval().
   * Zezwolenie tylko na zasoby z domeny firmowej i zaufanych CDN (np. Google Fonts).
2. **Dodatkowe nagłówki**:
   * **X-Content-Type-Options: nosniff** – blokada MIME-sniffingu.
   * **X-Frame-Options: DENY** – ochrona przed clickjackingiem.
   * **Referrer-Policy: strict-origin-when-cross-origin**.

§ 16.6. Logowanie i monitoring

1. **Zakres logowania**:
   * Wszystkie próby logowania (udane/nieudane), zmiany hasła, operacje krytyczne (np. eksport danych).
   * Pełne dzienniki błędów (stack trace) dostępne tylko dla ASI.
2. **Retencja logów**:
   * Logi przechowywane przez **12 miesięcy** w zaszyfrowanym repozytorium (AES-256).
   * Archiwizacja tygodniowa na osobnym serwerze.
3. **Narzędzia monitorujące**:
   * **OWASP ZAP** do skanowania podatności.
   * **ELK Stack** (Elasticsearch, Logstash, Kibana) do analizy logów w czasie rzeczywistym.

§ 16.7. Testy i audyty

1. **Testy penetracyjne**:
   * Przeprowadzane co **6 miesięcy** przez certyfikowane firmy zewnętrzne (np. Securitum).
   * Raporty z testów udostępniane Dyrektorowi Biura.
2. **Przegląd kodu**:
   * Code review pod kątem bezpieczeństwa przed każdym wdrożeniem.
   * Automatyczne skanowanie kodu narzędziami **SonarQube** i **Checkmarx**.
3. **Aktualizacje zależności**:
   * Cotygodniowe skanowanie bibliotek pod kątem luk (np. **Dependabot**).
   * Krytyczne aktualizacje wdrażane w ciągu **48 godzin**.

§ 16.8. Zarządzanie incydentami

1. **Procedura reagowania**:
   * Wykrycie podatności = natychmiastowe wyłączenie zagrożonej funkcjonalności.
   * Powiadomienie klientów w ciągu **24 godzin** w przypadku wycieku danych.
2. **Backup i odtwarzanie**:
   * Codzienne backupowanie bazy danych portalu (RPO = 1 dzień).
   * Testy odtwarzania danych co **3 miesiące**.

§ 16.9. Edukacja użytkowników

1. **Wytyczne dla klientów**:
   * Poradnik tworzenia silnych haseł dostępny na stronie logowania.
   * Powiadomienia o podejrzanych aktywnościach (np. logowanie z nowego kraju).
2. **Szkolenia pracowników**:
   * Warsztaty z bezpiecznego kodowania dla developerów co **kwartał**.
   * Symulacje ataków phishingowych dla księgowych co **2 miesiące**.

Rozdział 17. Monitorowanie bezpieczeństwa IT

1. Wszystkie zasoby IT Biura Księgowego podlegają monitorowaniu w celu zapewnienia bezpieczeństwa danych klientów oraz ciągłości działania usług. Za nadzór nad monitorowaniem odpowiedzialni są Administratorzy Systemów Informatycznych (ASI).
2. Każdy zasób IT (serwer główny, serwer archiwum, portal klienta, sieć LAN/WiFi, urządzenia pracowników zdalnych) musi mieć przypisaną klasyfikację bezpieczeństwa:

* **Klasa A**: Bazy danych klientów i serwer archiwum (dostęp ograniczony do wyznaczonego personelu),
* **Klasa B**: Narzędzia księgowe oraz systemy wewnętrzne,
* **Klasa C**: Sieć WiFi dla gości i zasoby publiczne.

Klasyfikacja ta definiuje poziom monitorowania, progi alarmowe i sposób obsługi zdarzeń.

1. **Zmiany konfiguracji**, instalacje oprogramowania oraz działania związane z monitoringiem muszą być zgodne z wewnętrzną Polityką Bezpieczeństwa Informacji (PBI).
2. **Zakres monitorowania obejmuje:** 4.1. Przypadki naruszenia poufności, integralności i dostępności danych (np. nieautoryzowany dostęp do bazy danych klientów),  
    4.2. Nieautoryzowane próby logowania lub nadania uprawnień,  
    4.3. Nietypowe działania systemów (np. wysoki transfer danych nocą),  
    4.4. Spadki wydajności usług (np. przeciążenie portalu klienta),  
    4.5. Wady oprogramowania lub błędne konfiguracje systemowe.
3. **Wykryte zdarzenia** muszą być analizowane i obsługiwane zgodnie z „Procedurą zarządzania incydentami bezpieczeństwa” obowiązującą w Biurze. Incydenty obejmują też potencjalne wycieki danych lub nieautoryzowany transfer danych klientów.
4. **Wyłączenie monitorowania** zasobu IT może nastąpić tylko w następujących przypadkach:  
    6.1. Wycofania zasobu z użycia,  
    6.2. Zmiany jego klasyfikacji bezpieczeństwa zatwierdzonej przez właściciela systemu,  
    6.3. Na podstawie pisemnej decyzji Dyrektora Biura Księgowego.
5. **Rejestracja zdarzeń** musi spełniać następujące standardy:  
    7.1. Dzienniki nie mogą ulegać przepełnieniu; dane logów muszą być regularnie archiwizowane,  
    7.2. Logi muszą być przechowywane na serwerze centralnym (zaleca się osobną partycję NTFS z ograniczonym dostępem),  
    7.3. Logi krytyczne przechowywane są przez 2 lata, a operacyjne przez 1 rok,  
    7.4. Dane w logach muszą być szyfrowane (np. AES-256) zarówno w transmisji, jak i przechowywaniu.
6. **Zdarzenia** muszą być monitorowane:  
    8.1. Manualnie przez administratora (przegląd logów co tydzień),  
    8.2. Automatycznie — narzędzia monitorujące powiadamiają ASI o krytycznych zdarzeniach (np. nieautoryzowany dostęp, ransomware).
7. **Decyzje** dotyczące polityk monitorowania i reagowania zatwierdza Dyrektor Biura Księgowego.

Rozdział 18. Bezpieczeństwo środowisk zwirtualizowanych

1. Środowiska zwirtualizowane w biurze księgowym składają się z dwóch podstawowych komponentów, którym należy zapewnić ochronę:  
    1.1. host wirtualizacyjny (serwer główny) – serwer umożliwiający uruchamianie maszyn wirtualnych obsługujących portal klienta, bazy danych oraz archiwum dokumentów,  
    1.2. maszyna wirtualna – środowisko z systemem operacyjnym do obsługi programów księgowych i baz danych, z kontrolą dostępu do zasobów sprzętowych i danych klientów.
2. Serwer główny i system storage muszą znajdować się w zamykanym pomieszczeniu biura z kontrolą dostępu (system kart pracowniczych) oraz rozliczalnością dostępu.
3. Narzędzia do zarządzania wirtualizacją i maszynami wirtualnymi powinny być chronione poprzez kontrolę ruchu sieciowego i działać w odseparowanej sieci LAN przeznaczonej tylko dla pracowników biura.
4. Zdalny dostęp do systemów (np. dla księgowych pracujących zdalnie) musi być realizowany przez szyfrowane połączenia VPN z obustronnym uwierzytelnianiem. Certyfikaty „self-signed” mogą być używane wyłącznie w środowisku testowym.
5. Konfiguracja hosta wirtualizacyjnego podlega takim samym wymaganiom bezpieczeństwa jak serwery opisane w § 19 „Bezpieczeństwo serwerów”.
6. W przypadku „utwardzania” wirtualizatora należy dodatkowo:  
    6.1. ograniczyć możliwość nadmiernego użycia zasobów przez pojedyncze maszyny wirtualne oraz wyłączyć współdzielenie schowka (clipboard) między maszyną fizyczną a wirtualną,  
    6.2. zabezpieczyć fizyczny serwer przed nieautoryzowanym dostępem do plików maszyn wirtualnych, które zawierają dane klientów.

**Rozdział 19. Bezpieczeństwo serwerów**

1. W Biurze Księgowym funkcjonuje pięć serwerów, podzielonych zgodnie z przeznaczeniem:
   * **Serwer główny** – przechowuje dane klientów, faktury oraz dane robocze księgowych.
   * **Dwa serwery zapasowe** – replikują dane z serwera głównego (failover i HA).
   * **Serwer archiwalny** – przechowuje dane archiwalne (do 10 lat).
   * **Zapasowy serwer archiwalny** – synchronizowany automatycznie z serwerem archiwalnym.
2. **Redundancja danych**:
   * Żadna baza danych nie jest przechowywana w jednym miejscu.
   * Przynajmniej jedna kopia wszystkich baz danych znajduje się w odseparowanej lokalizacji (np. chmura z szyfrowanym dostępem).
3. **System operacyjny i oprogramowanie zabezpieczające**:
   * Wszystkie serwery działają na systemie **Ubuntu Server**.
   * Oprogramowanie antywirusowe (np. ClamAV) jest zalecane, ale nieobowiązkowe – stosowane zgodnie z analizą ryzyka.
4. **Zasady funkcjonalne serwerów**:

* Serwery udostępniają wyłącznie te usługi i zasoby, które są niezbędne do realizacji ich funkcji w systemie IT.
* Zabronione jest uruchamianie usług zbędnych (np. usług współdzielenia plików, zdalnego pulpitu itp.).

1. **Dostęp zdalny**:
   * Zdalny dostęp dopuszczony wyłącznie przez szyfrowane połączenia (np. SSH z kluczem + certyfikat, VPN z 2FA).
   * Wymagane jest silne uwierzytelnianie dwustronne.
2. **Granulacja uprawnień administratora**:

* Role administratora podzielone na cztery typy czynności:
  + 1. Zarządzanie użytkownikami i uprawnieniami.
    2. Zarządzanie systemem operacyjnym serwera.
    3. Administracja bazą danych i aplikacjami.
    4. Audyt i analiza logów bezpieczeństwa.
  + W firmie, ze względu na małą liczbę pracowników, wszystkie te role pełni jedna kompetentna osoba (ASI), z obowiązkiem stosowania zasady wiedzy koniecznej.

**Rozdział 20. Bezpieczeństwo środowiska IT**

1. Ochronie podlegają wszystkie komponenty środowiska IT, w tym:

* Komputery i urządzenia pracowników,
* Serwery lokalne i wirtualne,
* Środowiska chmurowe,
* Aplikacje księgowe i bazy danych.

1. Zabezpieczenia środowiska IT obejmują:
   * **Firewall z segmentacją sieci** (LAN, Wi-Fi dla gości, VPN),
   * **Koncentrator VPN** z obustronnym uwierzytelnianiem,
   * **Systemy AV/EDR** (np. ClamAV, opcjonalnie),
   * **IPS/IDS** do detekcji włamań,
   * **Mechanizmy DLP** w aplikacjach przetwarzających dane klientów,
   * **Monitoring sieci (Network Forensics)** dla wykrywania anomalii,
   * **System SIEM** do analizy logów,
   * **Sandbox** do analizy podejrzanych załączników.
2. Wdrożone komponenty bezpieczeństwa działają w **wydzielonych segmentach sieci**, zgodnie z klasyfikacją zasobów (A, B, C).
3. Wszystkie zmiany konfiguracji i aktualizacje zabezpieczeń:
   * Muszą być przetestowane w środowisku testowym.
   * Nie mogą naruszać zasad Polityki Bezpieczeństwa Informacji (PBI).

**Rozdział 21. Edukacja i świadomość bezpieczeństwa IT**

1. Obowiązkowe szkolenia z zakresu bezpieczeństwa IT obejmują:
   * Wszystkich pracowników Biura, w szczególności 4 księgowych oraz osoby odpowiedzialne za dane klientów.
2. Zakres edukacji obejmuje:
   * Aktualne zagrożenia (phishing, ransomware, inżynieria społeczna),
   * Procedury postępowania w przypadku incydentu (np. podejrzenie wycieku danych),
   * Obowiązki wynikające z przepisów prawnych (RODO, Ustawa o rachunkowości),
   * Praktyczne zasady bezpiecznej pracy (hasła, MFA, dostęp do danych klientów).
3. Forma szkoleń:
   * E-learning, warsztaty, prezentacje stacjonarne lub online,
   * Symulacje incydentów (np. kampanie phishingowe).
4. Częstotliwość:
   * Szkolenia obowiązkowe co najmniej raz w roku,
   * Dodatkowe warsztaty dla księgowych co 2 miesiące (dot. phishingu),
   * Techniczne szkolenia dla administratora systemów – zgodnie z potrzebą.
5. Odpowiedzialność:
   * Organizacja i nadzór: Właściciel lub Kierownik Biura.
   * Nadzór merytoryczny: Administrator Bezpieczeństwa Informacji (ABI).
6. Dokumentacja:
   * Każde szkolenie potwierdzane listą obecności lub potwierdzeniem ukończenia kursu.
   * ABI prowadzi rejestr szkoleń i harmonogram działań edukacyjnych.