

Spis treści

1. Wprowadzenie	7
1.1. Znaczenie bezpieczeństwa w biurze rachunkowym	7
1.2. Bezpieczeństwo i poufność danych finansowych klientów	9
2. Zarządzanie ryzykiem i ubezpieczenia	10
2.1. Analiza ryzyka dla biura rachunkowego	10
2.1.1. Czym jest ryzyko?	10
2.1.2. Identyfikacja i ocena ryzyk	15
2.2. Sposoby ograniczenia ryzyka	16
2.2.1. Eliminacja lub redukcja ryzyka	16
2.2.2. Przeniesienie ryzyka	17
2.2.3. Akceptacja i monitorowanie ryzyka	17
2.3. Oferty ubezpieczeniowe dostępne na rynku	18
3. Umowa o świadczenie usług księgowych i zakres odpowiedzialności	20
3.1. Ryzyka prawne związane z wykonywaniem usług księgowych	20
3.1.1. Rodzaje ryzyk prawnych	21
3.1.1.1. Ryzyko cywilnoprawne	21
3.1.1.2. Ryzyko publicznoprawne	23
3.1.1.3. Ryzyko karne	25
3.1.1.4. Ryzyko prawnopracownicze	27
3.2. Ustalenie zakresu i zasad współpracy	30
3.2.1. Zasady tworzenia umowy świadczenia usług księgowych	31
3.2.2. Zarządzanie odpowiedzialnością	32
3.3. Odpowiedzialność za obliczanie zaliczek na podatki i składki ZUS	36
3.4. Konsekwencje karne i karnoskarbowe	41
3.4.1. Wykonywanie obowiązków w zakresie rachunkowości	42
3.4.2. Odpowiedzialność karnoskarbowa	43
3.4.3. Odpowiedzialność karnoskarbowa za nieprowadzenie ksiąg podatkowych	49
4. Bezpieczeństwo fizyczne i przechowywanie dokumentów	51
4.1. Zasady bezpiecznego przechowywania dokumentów finansowych klientów	51
4.2. Zabezpieczenie pomieszczeń i sprzętu przed kradzieżą, uszkodzeniami i zagrożeniami zewnętrznymi	54
4.2.1. Odporność na włamanie	54
4.3. Monitoring, systemy alarmowe i inne działania prewencyjne	56
4.3.1. Monitoring wizyjny	56
4.3.2. Systemy alarmowe	58
4.3.3. Kontrola dostępu	59
4.3.4. Zabezpieczenia prewencyjne	60

4.3.5.	Integracja systemów	61
4.3.6.	Regularne przeglądy i aktualizacje	62
4.4.	Sposoby przechowywania danych z zastosowaniem zabezpieczeń fizycznych i elektronicznych	63
5.	Zabezpieczenie systemów informatycznych i kontrola dostępu	64
5.1.	Kompetencje IT	64
5.1.1.	Opcje zarządzania IT w biurze rachunkowym	65
5.1.1.1.	Właściciel jako osoba odpowiedzialna za IT	65
5.1.1.2.	Wykwalifikowany pracownik biura rachunkowego	66
5.1.1.3.	Zewnętrzny specjalista IT „na wezwanie”	67
5.1.1.4.	Firma oferująca kompleksowe usługi IT	68
5.1.2.	Zalety i wady różnych opcji zarządzania IT	69
5.1.2.1.	Analiza kosztów	69
5.1.2.2.	Dostępność i czas reakcji	70
5.1.2.3.	Poziom kompetencji i doświadczenie	71
5.1.3.	Współpraca z zewnętrznymi dostawcami usług IT	72
5.1.3.1.	Wybór odpowiedniego dostawcy	72
5.1.3.2.	Umowy i regulacje prawne	73
5.1.3.3.	Zarządzanie ryzykiem i ochrona danych klienta	74
5.1.4.	Reagowanie na incydenty związane z IT	75
5.1.4.1.	Planowanie odpowiedzi na incydenty	75
5.1.4.2.	Analiza przyczyn i lekcje wyniesione z incydentów	75
5.1.4.3.	Komunikacja z klientami i partnerami w przypadku incyduentu	75
5.2.	Narzędzia i metody zabezpieczenia systemów informatycznych, które powinno stosować biuro rachunkowe	76
5.2.1.	Wybór odpowiedniego oprogramowania zabezpieczającego	76
5.2.1.1.	Analiza dostępnych opcji	76
5.2.1.2.	Znaczenie aktualizacji oprogramowania	77
5.2.2.	Zapobieganie atakom phishingowym	77
5.2.2.1.	Edukacja pracowników na temat zagrożeń	77
5.2.2.2.	Przykłady typowych ataków i jak się przed nimi bronić	78
5.2.2.3.	Stosowanie oprogramowania do filtrowania wiadomości e-mail	78
5.2.3.	Aktualizacje i utrzymanie systemów	79
5.2.3.1.	Regularne aktualizacje systemu operacyjnego i oprogramowania	79
5.2.3.2.	Skanowanie w poszukiwaniu luk bezpieczeństwa	79
5.2.4.	Zabezpieczenie sieci biurowej	79
5.2.4.1.	Stosowanie firewalla	79
5.2.4.2.	Zabezpieczenie Wi-Fi	80
5.2.5.	Ochrona przed atakami typu ransomware	80
5.2.5.1.	Zapobieganie infekcji	80
5.2.5.2.	Tworzenie kopii zapasowych danych	80

5.2.5.3.	Jak postępować w przypadku ataku	80
5.2.6.	Ochrona urządzeń przenośnych	81
5.2.6.1.	Zabezpieczanie telefonów i tabletów	81
5.2.6.2.	Szyfrowanie danych na urządzeniach przenośnych	81
5.3.	Dobra kopia zapasowa	81
5.3.1.	Czym są kopie zapasowe i dlaczego są ważne	82
5.3.2.	Jakie wymagania musi spełniać kopia zapasowa	82
5.3.3.	Regularne testowanie kopii zapasowych	82
5.4.	Autoryzacja dostępu, silne hasła i menedżery haseł	83
5.4.1.	Autoryzacja dostępu	83
5.4.1.1.	Uwierzytelnianie jednoskładnikowe	84
5.4.1.2.	Uwierzytelnianie dwuskładnikowe	84
5.4.1.3.	Uwierzytelnianie wieloskładnikowe	84
5.4.2.	Silne hasła	84
5.4.2.1.	Wskazówki dotyczące tworzenia silnych haseł	84
5.4.2.2.	Regularne aktualizowanie haseł i unikanie ich wielokrotnego stosowania	85
5.4.3.	Stosowanie menedżerów haseł	85
5.4.3.1.	Czym są menedżery haseł i dlaczego są ważne	85
5.4.3.2.	Bezpieczne przechowywanie i zarządzanie hasłami za pomocą menedżerów	86
5.4.3.3.	Synchronizacja haseł pomiędzy różnymi urządzeniami	86
5.5.	Praca zdalna i dodatkowe środki bezpieczeństwa	86
5.5.1.	Wprowadzenie do pracy zdalnej w biurze rachunkowym	86
5.5.1.1.	Dlaczego praca zdalna stała się popularna	86
5.5.1.2.	Wykorzystanie pracy zdalnej w biurach rachunkowych	86
5.5.2.	Wyzwania związane z pracą zdalną	87
5.5.2.1.	Problemy związane z bezpieczeństwem danych	87
5.5.2.2.	Zarządzanie zespołem pracującym zdalnie	87
5.5.2.3.	Komunikacja z klientami na odległość	87
5.5.3.	Środki bezpieczeństwa dla pracy zdalnej	88
5.5.3.1.	Bezpieczne połączenia VPN i szyfrowanie danych	88
5.5.3.2.	Korzystanie z autoryzacji wieloskładnikowej	88
5.5.3.3.	Ograniczanie dostępu do poufnych danych tylko dla uprawnionych pracowników	88
5.5.4.	Sprzęt i oprogramowanie do pracy zdalnej	88
5.5.4.1.	Praca na własnym sprzęcie	88
5.5.4.2.	Wybór odpowiednich urządzeń i oprogramowania	89
5.5.4.3.	Ochrona sprzętu przed zagrożeniami fizycznymi	89
5.6.	Sposoby kontroli dostępu do poufnych danych finansowych klientów	90
5.6.1.	Dlaczego kontrola dostępu jest ważna	90
5.6.2.	Rola autoryzacji w kontroli dostępu	90
5.6.3.	Stosowanie zasad minimalnych uprawnień i segregacji obowiązków	91

5.6.3.1. Implementacja zasady najmniejszych uprawnień w praktyce	91
5.6.4. Systemy do zarządzania tożsamościami i dostępem	91
5.6.4.1. Praktyka w biurach rachunkowych	91
5.6.5. Monitorowanie i audyt dostępu	92
5.6.5.1. Reagowanie na nieautoryzowany dostęp	92
6. Sposoby przechowywania danych z zastosowaniem zabezpieczeń fizycznych i elektronicznych	92
6.1. Małe biuro	93
6.1.1. Zabezpieczenie fizyczne w małym biurze	93
6.1.2. Zabezpieczenia elektroniczne w małym biurze	94
6.2. Średnie biuro	94
6.2.1. Zabezpieczenie fizyczne w średnim biurze	95
6.2.2. Zabezpieczenia elektroniczne w średnim biurze	95
6.3. Duże biuro	96
6.3.1. Zabezpieczenie fizyczne w dużym biurze	96
6.3.2. Zabezpieczenia elektroniczne w dużym biurze	97
6.4. Antyprzykład – nieprawidłowe zabezpieczenia biura	97
6.4.1. Zabezpieczenie fizyczne – antyprzykład i propozycje usprawnień	97
6.4.2. Zabezpieczenia elektroniczne – antyprzykład i propozycje usprawnień	98
7. Organizacja i procedury bezpieczeństwa	98
7.1. Procedury bezpieczeństwa, które powinno stosować biuro rachunkowe (RODO)	99
7.1.1. Przykłady procedur bezpieczeństwa w biurze rachunkowym	108
7.2. Procedury zwiększające poziom bezpieczeństwa	119
7.2.1. Procedury dotyczące fizycznego dostępu	120
7.2.2. Procedury IT dotyczące pracowników	122
7.2.3. Procedury IT dotyczące obsługi technicznej	123
7.3. Szkolenie pracowników w zakresie ochrony danych i procedur bezpieczeństwa	124
7.4. Bezpieczeństwo danych powierzonych podmiotom zewnętrznym	126
8. Audyty bezpieczeństwa i ciągłe doskonalenie	128
8.1. Korzyści z audytów	128
8.2. Przykładowe działania przeprowadzane podczas audytu bezpieczeństwa	129
8.2.1. Ocena zabezpieczeń fizycznych	129
8.2.2. Kontrola zabezpieczeń elektronicznych	129
8.2.3. Kontrola dostępu do danych	129
8.2.4. Analiza procedur reagowania na incydenty	130
8.2.5. Ocena szkoleń pracowników	130
Podsumowanie	131