Załącznik nr 9. Procedura zarządzania ryzykiem

Sposób oceny prawdopodobieństwa wystąpienia ryzyka:

Prawdopodobieństwo wystąpienia ryzyka	Ilość punktów	Przesłanki
wysokie	3	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się wielokrotnie w ciągu roku.
średnie	2	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się kilkakrotnie w ciągu roku.
niskie	1	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub nie zdarzy się w ciągu roku.

Sposób oceny skutku ryzyka:

Skutek wystąpienia ryzyka	Ilość punktów	Przesłanki
wysokie	3	Poważne zagrożenie realizacji czynności Długotrwały i trudny proces przywracania stanu poprzedniego
średnie	2	Spadek efektywności działania i obniżenie jakości wykonywania zadań. Trudny proces przywracania stanu poprzedniego.
niskie	1	Zakłócenie lub opóźnienie w wykonywaniu zadań. Skutki łatwe do usunięcia.

Progi akceptowalności ryzyka	
1-2 ryzyko nieznaczne	akceptowalne
3-5 ryzyko umiarkowane	akceptowalne
6-9 ryzyko wysokie	niedopuszczalne

1.	2.	3.	4.	5.	6.
Lp	Rodzaj ryzyka	Prawdopodobieństwo wystąpienia ryzyka (od 1 do 3)	Skutek ryzyka w skali (od 1 do 3)	Wysokość ryzyka (iloczyn kolumn 5x6)	Środki techniczne i organizacyjne w celu zmniejszenia ryzyka
1.	Nieuprawniony dostęp do pomieszczenia, w którym są przetwarzane dane osobowe	2	1	2	- szkolenia dla pracowników - monitoring budynku - przechowywanie kluczy w zamkniętej kasetce
2.	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe	1	3	3	- okresowa zmiana haseł dostępu - rejestrowanie czynności prowadzonych na komputerze
3.	Utrata nośnika zawierającego dane osobowe	1	1	1	- okresowe archiwizowanie danych - zakup nowych nośników
4.	Nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym	1	1	1	- szkolenia dla pracowników
5.	Atak wirusa, włamanie do systemu komputerowego	3	1	3	- szkolenia dla pracowników - zabezpieczenie komputerów (program antywirusowy, firewall) - używanie tylko zaufanych programów pochodzących
6.	Klęska żywiołowa, wypadek, pożar, zalanie lub inne zdarzenie, w wyniku których utracono poufność danych osobowych	1	3	3	- okresowe próbne alarmy - wdrożenie odpowiednich procedur na wypadek

					zdarzeń losowych - okresowa archiwizacja danych
7.	Błędy i pomyłki użytkowników	3	1	3	- szkolenia pracowników - kontrola zarządcza - okresowy audyt
8.	Awaria sprzętu (w tym utrata dostaw prądu)	2	2	4	- okresowe przeglądy techniczne - stopniowa wymiana sprzętu - archiwizacja danych na nośnikach zewnętrznych - używanie UPS
9.	Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników	1	3	3	- trwałe usuwanie nośników danych przez wyspecjalizowane firmy
10.	Nieautoryzowane użycie urządzeń	1	3	3	- szkolenia pracowników - wymuszanie zmiany haseł dostępu - nadawanie unikalnych loginów i haseł użytkownikom
11.	Nielegalne przetwarzanie danych osobowych	1	3	3	- szkolenia pracowników - okresowy audyt przetwarzania danych (w tym dokumentów dane zawierających)