Załącznik nr 2: Arkusz analizy ryzyka
Administrator: Sądeckie Towarzystwo Muzyczne w Nowym Sączu

Arkusz analizy ryzyka

Pr-Prawdopodobieństwo wystąpienia zagrożenia [skala od 1 do 3]; His - ocena historyczna w ciągu ostatnich 5 lat [skala od 0 do 2]; Sk - potencjalne skutki wystąpienia zagrożenia [skala od 1 do 3]; Ryz - ryzyko wystąpienia zagrożenia (skala od 1 do 8), Wzór: Ryz = Pr + His + Sk

Zagrożenie	Opis zagrożenia	Pr	His	Sk	Ryz	Zabezpieczenie
nieuprawnione ujawnienie danych osobowych	1. Przekazanie danych osobom nieuprawnionym	2	0	1	**3**	Instrukcja zarządzania i regulamin ODO - elementy Polityki ochrony danych osobowych: ▪ zabezpieczenia fizyczne ▪ polityka kluczy ▪ polityka czystego biurka ▪ zasada bezpiecznego wygaszacza ekranu ▪ zabezpieczenia techniczne ▪ polityka haseł ▪ zasady tworzenia kopii zapasowych ▪ procedura utylizacji elektronicznych nośników danych i wydruków komputerowych ▪ procedura zabezpieczenia systemu informatycznego ▪ zasady wykonywania przeglądów i konserwacji ▪ zapoznawanie personelu z zasadami ochrony danych osobowych
	2. Przesłanie maila z danymi osobowymi do osób nieuprawnionych	2	0	2	**4**	
	3. Zagubienie/kradzież nośników papierowych i elektronicznych poza organizacją (dokumentów, laptopów, dysków przenośnych, pendrive)	1 2	0 0	2 2	**3** **4**	
	4. Zagubienie/kradzież sprzętu elektronicznego poza organizacją	1	0	2	**2**	
	5. Wyrzucenie niezniszczonych dokumentów	1	0	2	**2**	
	6. Utylizacja/sprzedaż/naprawa sprzętu z nieusuniętymi danymi osobowymi na nośnikach	1	0	2	**3**	
nieuprawniony dostęp do danych osobowych podczas przesyłania ich za pomocą środków elektronicznych	„Podsłuch" przesyłanych danych podczas korzystania z aplikacji, maila oraz formularzy kontaktowych	1	0	1	2	Instrukcja zarządzania i regulamin ODO - elementy Polityki ochrony danych osobowych: ▪ procedura zabezpieczenia systemu informatycznego ▪ program antywirusowy zapory systemowe ▪ korzystanie wyłącznie z legalnego oprogramowania
	Zainfekowanie komputera wirusem lub innym szkodliwym oprogramowaniem	1	1	1	3	
nieuprawniony dostęp do danych osobowych podczas przechowywania	1. Niezabezpieczony dostęp do pomieszczeń z dokumentacją papierową i sprzętem komputerowym (biuro, archiwum, szafy)	1	0	2	2	Instrukcja zarządzania i regulamin ODO - elementy Polityki ochrony danych osobowych: ▪ zabezpieczenia fizyczne ▪ polityka kluczy ▪ polityka czystego biurka ▪ zasada bezpiecznego wygaszacza ekranu ▪ zabezpieczenia techniczne ▪ polityka haseł ▪ zasady tworzenia kopii zapasowych ▪ procedura utylizacji elektronicznych nośników danych i wydruków komputerowych ▪ procedura zabezpieczenia systemu informatycznego ▪ zasady wykonywania przeglądów i konserwacji ▪ zapoznawanie personelu z zasadami ochrony danych osobowych ▪ prowadzenie polityki upoważnień/odwołania upoważnień i ewidencji osób upoważnionych ▪ ewidencja osób posiadających klucze do biura
	2. Niezabezpieczony dostęp do baz danych lub do katalogów z plikami zawierającymi dane osobowe	2	0	2	4	

Załącznik nr 2: Arkusz analizy ryzyka
Administrator: Sądeckie Towarzystwo Muzyczne w Nowym Sączu

przypadkowe lub niezgodne z prawem zniszczenie, uszkodzenie danych osobowych	1. Pożar, 2. Zalanie, 3. Awarie sprzętu komputerowego 4. Awarie oprogramowania 5. Błędy w działaniu systemów i aplikacji (np. na skutek aktualizacji, „konfliktu" programów) 6. Brak dostępu do Internetu	1 1 1 1 1 1	0 0 0 0 0 1	2 1 1 1 1 1	3 2 2 2 2 3	Instrukcja zarządzania i regulamin ODO - elementy Polityki ochrony danych osobowych: ▪ zabezpieczenia fizyczne ▪ gaśnica na korytarzu ▪ zakaz palenia tytoniu w biurze ▪ zabezpieczenia techniczne ▪ polityka haseł ▪ zasady tworzenia kopii zapasowych ▪ procedura zabezpieczenia systemu informatycznego ▪ zasady wykonywania przeglądów i konserwacji ▪ zapoznawanie personelu z zasadami ochrony danych osobowych
przypadkowe lub niezgodne z prawem utracenie danych	1. Atak hakerski 2. Brak kopii bezpieczeństwa lub kopie niemożliwe do odtworzenia	2 1	0 0	1 1	2 2	▪ procedura zabezpieczenia systemu informatycznego ▪ zasady tworzenia kopii zapasowych
nieuprawniony dostęp do pomieszczeń administratora	1. włamanie się do biura 2. niezabezpieczony dostęp do pomieszczeń z dokumentacją papierową i sprzętem komputerowym (biura, archiwum)	1 1	0 0	1 1	2 2	▪ zabezpieczenia fizyczne ▪ polityka kluczy ▪ umiejscowienie biura na I piętrze ▪ szafy zamykane na klucz ▪ budynek w którym znajduje się biuro zamykane po godz. 19, ▪ zapoznawanie personelu z zasadami ochrony danych osobowych ▪ prowadzenie polityki upoważnień/odwołania upoważnień i ewidencji osób upoważnionych. ▪ ewidencja osób posiadających klucze do biura ▪ zabezpieczenie komputerów
Kradzież/zagubienie sprzętu i nośników poza organizacją	Kradzież/zgubienie nośników danych niezabezpieczonych hasłem lub programem kryptograficznycm	1	0	2	3	▪ zakaz wynoszenia na zewnątrz niezaszyfrowanych nośników z danymi osobowymi (np. przenośnych dysków twardych, pen-drive, płyt CD, DVD)
Nieprzestrzeganie zasad ochrony danych przez personel administratora	Niestosowanie się przez personel do Polityki ochrony danych osobowych	1	0	2	3	▪ regulamin ochrony danych osobowych, ▪ procedura podpisywania oświadczeń o poufności i zobowiązaniu do stosowania zasad ochrony danych; ▪ odpowiedzialność personelu wynikająca z przepisów prawa i stosunków łączących z administratorem (personel jest z tymi zasadami zapoznawany), ▪ kontrole prowadzone przez administratora w zakresie stosowania procedur ochrony danych osobowych
inne	Nie dotyczy					▪ nie dotyczy