SZKOŁA PODSTAWOWA Nr 2
im. Ks. Jana Twardowskiego
ul. Boh. Monte Cassino 25
15-873 Białystok
tel. 85 742 03 04
Reg. 000735227, NIP 542-20-73-403

Analiza ryzyka dla procesu –

Obsługa i prowadzenie korespondencji za pomocą skrzynki do e-Doręczeń

I. Kontekst

Doręczanie pism drogą elektroniczną reguluje ustawa dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U.2024.1045 t.j. z dnia 2024.07.16). W tej formie komunikacji tak samo jak i w korespondencji w formie papierowej dochodzić będzie do przetwarzania danych osobowych. Przepisy RODO nakładają na administratorów m.in. obowiązek przetwarzania danych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Jest to naczelna zasada przetwarzania na podstawie RODO – zasada integralności i poufności (art. 5 ust. 1 lit. f RODO).

II. Cel

Doręczenia elektroniczne to cyfrowa komunikacja obywateli i przedsiębiorców z podmiotami publicznymi. Zgodnie z informacjami podawanymi przez Ministerstwo Cyfryzacji usługa ta ma być:

- przyjazna i bezpieczna,
- równoważna prawnie z przesyłką poleconą za zwrotnym potwierdzeniem odbioru lub z doręczeniem osobistym,
- niezawodna dzięki dostawcy usługi rejestrowanego doręczenia elektronicznego (trzecia zaufana strona),
- interoperacyjna (zgodna z wymaganiami rozporządzenia Parlamentu Europejskiego – eIDAS i unijnym Planem działań na rzecz administracji elektronicznej 2020 – Tallinn Declaration on eGoverment 2017 r.).

W ramach e - Doręczeń będzie możliwa także usługa hybrydowa za pomocą, której podmioty publiczne będą mogły komunikować się z osobami wykluczonymi cyfrowo. Osobom tym umożliwi się odbiór korespondencji w sposób tradycyjny, mimo że w urzędzie dokumenty będą zapisane cyfrowo.

III. Analiza ryzyka - metodyka

1. Analiza zidentyfikowanego ryzyka polega na oszacowaniu:
   a) **P**rawdopodobieństwa jego wystąpienia – ocena punktowa w skali 1 – 4
   b) **S**kutku jego ewentualnego wystąpienia – ocena punktowa w skali 1 – 4
2. Sposób oceny prawdopodobieństwa wystąpienia oraz skutków ryzyka przedstawiają odpowiednio **tabela nr 1 i tabela nr 2**

Tabela nr 1 - Sposób oceny prawdopodobieństwa wystąpienia ryzyka

Prawdopodobieństwo wystąpienia ryzyka	Ilość punktów	Przesłanki
Bardzo wysokie (81-100%)	4	Przewiduje się, że zdarzenie z pewnością wystąpi w ciągu roku
Wysokie (61-80%)	3	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się wielokrotnie w ciągu roku
Średnie (21-60%)	2	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub kilka razy w ciągu roku

Niskie (0-20%)	1	Przewiduje się, że zdarzenie objęte ryzykiem, zdarzy się raz lub nie zdarzy się w ciągu roku

Tabela nr 2 - Sposób oceny skutku ryzyka

Skutek wystąpienia ryzyka*	Ilość punktów	Przesłanki
Bardzo wysoki	4	Zdarzenie wywołuje bardzo wysoki skutek. Skutki mogą prowadzi do wysokiego uszczerbku fizycznego, szkód majątkowych dla osób fizycznych. Zagrożenie ustawową karą pozbawienia wolności. Bardzo wysokie koszty wielu procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Kontrole organów ścigania. Zdarzenie objęte ryzykiem powoduje brak realizacji kluczowych zadań albo osiąganie założonych celów – poważny uszczerbek w zakresie jakości wykonywanych zadań, poważna strata finansowa albo reputacji. Z wystąpieniem zdarzenia objętego ryzykiem wiąże się długotrwały i trudny proces przywracania stanu poprzedniego.
Wysoki	3	Zdarzenie wywołuje wysoki skutek. Skutki mogą prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych dla osób fizycznych. Zdarzenie powoduje np. wysokie ustawowe kary pieniężne dla jednostki. Koszt kilku procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Kontrole i kary UODO. Zdarzenie objęte ryzykiem powoduje znaczącą stratę posiadanych zasobów, ma negatywny wpływ na wykonywanie zadań. Wpływa negatywnie na reputację jednostki. Skutki zdarzenia wiążą się z trudnym procesem przywracania stanu poprzedniego.
Średni	2	Zdarzenie wywołuje średni skutek. Może spowodować nałożenie kar ustawowych w dolnej granicy kary. Koszt nielicznych procesów sądowych (obsługa prawna, informacyjna, odszkodowania). Zdarzenie objęte ryzykiem powoduje niewielką stratę finansową, niewielkie zakłócenie lub opóźnienie w wykonywaniu zadań. Niski wpływ na reputacje jednostki. Skutki zdarzenia można łatwo usunąć.
Niski	1	Zdarzenie wywołuje niski skutek. Nie skutkuje poważnym wpływem na prawa i wolności osób fizycznych np. nie grozi dyskryminacją, kradzieżą tożsamości, oszustwem spowodowanym kradzieżą tożsamości. Zdarzenie objęte ryzykiem powoduje minimalną stratę finansową lub krótkotrwałe zakłócenia lub opóźnienie w wykonywaniu zadań. Nie wpływa na reputację. Skutki zdarzenia można łatwo usunąć

3. Punktowa **istotność ryzyka** (Istotność) określana jest według wzoru:

   Istotność = **P**rawdopodobieństwo x **S**kutek

4. Poziomy istotności ryzyka (dopuszczalność ryzyka) przedstawia **tabela nr 3**

Tabela nr 3 - Poziomy Istotności ryzyka

Oszacowanie ryzyka	Dopuszczalność ryzyka	Działania
Ryzyko poważne Skala: 13 - 16 pkt.	Niedopuszczalne (nieakceptowane)	Działania nie mogą być podjęte ani kontynuowane do czasu zmniejszenia ryzyka do poziomu dopuszczalnego
Ryzyko wysokie Skala: 9 – 12 pkt.	Dopuszczalne (akceptowane)	Zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane zmniejszenie ryzyka
Ryzyko umiarkowane Skala: 5 - 8 pkt.	Dopuszczalne (akceptowane)	Zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane i skuteczne zmniejszenie ryzyka
Ryzyko nieznaczne Skala: 1- 4 pkt.	Dopuszczalne (akceptowane)	Zaleca się rozważenie możliwości dalszego zmniejszenia poziomu ryzyka lub zapewnienie, że ryzyko pozostanie na tym samym poziomie

Tabela nr 4 – Analiza ryzyka

Zagrożenie (źródło ryzyka)	Zagrożony atrybut: poufność/integralność/dostępność	Skutki wystąpienia ryzyka	Prawdopodobieństwo	Skutki	Poziom istotności ryzyka	Środki techniczne i organizacyjne redukujące ryzyko	Decyzja dotycząca ryzyka
Ataki hakerskie	Poufność	• wyciek danych osobowych • kradzież tożsamości • szkody finansowe	2	3	6	• wdrożenie silnych zabezpieczeń sieciowych i firewalli • wymuszenie używania silnych haseł i autoryzacji dwuetapowej • regularne szkolenia w zakresie ochrony danych dla personelu • regularne szkolenia pracowników z zakresu cyberbezpieczeństwa	**Akceptacja**
Wyciek danych	Poufność	• dostęp osób trzecich do danych osobowych • kradzież tożsamości • możliwość zapoznania się z danymi z art. 9 ust. 1 RODO • utrata zaufania do podmiotu przetwarzającego dane w systemie elektronicznym	2	3	6	• wdrożenie silnych zabezpieczeń sieciowych i firewalli • wymuszenie używania silnych haseł i autoryzacji dwuetapowej • regularne szkolenia	**Akceptacja**

						w zakresie ochrony danych dla personelu • regularne szkolenia pracowników z zakresu cyberbezpieczeństwa	
Braki w zabezpieczeniach sieciowych	Poufność Integralność Dostępność	• próby ujawnienia wrażliwych danych • modyfikacja lub odmowa dostępu do usług • kradzież danych	2	4	8	• implementacja funkcji kontroli dostępu • szyfrowanie danych • zapory sieciowe • systemy wykrywania włamań • oraz systemy zapobiegania włamaniom • regularne przeglądy stosowanych zabezpieczeń • zabezpieczenie środków finansowych na nowe technologie mające wpływ na bezpieczeństwo sieci	**Akceptacja**
Brak nadzoru nad sprzętem komputerowym podczas pracy zdalnej	Poufność Integralność	• dostęp osób trzecich do danych osobowych • możliwość modyfikacji treści dokumentu	2	2	4	• indywidualny login oraz hasło dostępu do systemu • wygaszacz ekranu włączający się po	**Akceptacja**

						kilku minutach bezczynności • szkolenia pracowników z zasad ochrony danych podczas pracy zdalnej • regulamin pracy zdalnej	
Brak nadzoru nad dokumentacją podczas pracy zdalnej	Poufność Integralność	• dostęp osób trzecich do danych osobowych • możliwość fizycznego zniszczenia dokumentacji papierowej	2	2	4	• ewidencja dokumentacji • przechowywanie dokumentacji przez okres niezbędny do wykonania zadania • zakaz wynoszenia oryginałów dokumentacji • zakaz niszczenia dokumentacji w domu • ograniczenie drukowania dokumentacji w domu • procedura postępowania z dokumentacją papierową	**Akceptacja**

Brak szkoleń pracowników z usługi e – Doręczeń	Poufność	• doręczenie przesyłki innej osobie w wyniku błędnej weryfikacji podmiotu danych • brak weryfikacji czy dany podmiot posiada skrzynkę do e-doręczeń • niedostosowanie dokumentu do wymagań technicznych e-doręczenia	3	2	6	• regularne szkolenia pracowników • obowiązkowe szkolenia dla nowoprzyjętych pracowników	**Działanie: przeprowadzenie szkolenia**

Dyrektor
Szkoły Podstawowej Nr 2
im. ks. Jana Twardowskiego
w Białymstoku

10.02.2025 mgr Halina Puchalska

Data i podpis Administratora