

**Obowiązuje od 10 kwietnia 2026 roku**

**Polityka świadczenia usługi i deklaracja praktyk  
dla usługi rejestrowanego doręczenia elektronicznego  
w Poczcie Polskiej S.A.**

wersja 5.0

## Metryka dokumentu

<b>Nazwa:</b>	Polityka świadczenia usługi i deklaracja praktyk dla usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A.		
<b>Identyfikator dokumentu</b>			
<b>Wersja:</b>	5.0	<b>Autor:</b>	Poczta Polska S.A.
<b>Stron:</b>	29	<b>Data:</b>	02.04.2026

## Lista dystrybucyjna

Imię i nazwisko albo opis stanowiska	Imię i nazwisko albo opis stanowiska
1.	7.
2.	8.
3.	9.
4.	10.
5.	11.
6.	12.

## Akceptacja ostatniej wersji

Rodzaj kontroli / stanowisko	Imię i nazwisko	Data i podpis

<b>1. Wstęp .....</b>	<b>6</b>
<b>1.1. Wprowadzenie .....</b>	<b>6</b>
<b>1.2. Słownik .....</b>	<b>6</b>
<b>1.3. Definicje Stron Usługi RDE PP .....</b>	<b>8</b>
<b>1.4. Zakres Usługi RDE PP .....</b>	<b>9</b>
<b>1.5. Podstawowe elementy Usługi RDE PP .....</b>	<b>9</b>
<b>2. Administracja i repozytorium.....</b>	<b>10</b>
<b>2.1. Administracja Polityką.....</b>	<b>10</b>
<b>2.2. Repozytorium i publikacja dokumentu .....</b>	<b>10</b>
<b>3. Identyfikacja i uwierzytelnienie .....</b>	<b>11</b>
<b>4. Zabezpieczenia organizacyjne, operacyjne i fizyczne .....</b>	<b>12</b>
<b>4.1. Zabezpieczenia fizyczne .....</b>	<b>12</b>
4.1.1. Lokalizacja i budynki .....	12
4.1.2. Dostęp fizyczny .....	12
4.1.3. Bezpieczeństwo środowiskowe .....	12
4.1.4. Nośniki informacji.....	13
4.1.5. Niszczenie informacji .....	13
4.1.6. Kopie bezpieczeństwa .....	13
<b>4.2. Zabezpieczenia organizacyjne .....</b>	<b>13</b>
4.2.1. Role zaufane .....	13
4.2.2. Role zaufane podlegające separacji obowiązków .....	15
4.2.3. Zarządzanie incydentami .....	15
4.2.4. Zarządzanie ryzykiem .....	15
4.2.5. Nadzór nad Personelem pełniącym Role zaufane .....	15
4.2.5.1. Kwalifikacje, doświadczenie, upoważnienia .....	15
4.2.5.2. Weryfikacja Personelu .....	16
4.2.5.3. Szkolenia .....	16
4.2.5.4. Sankcje z tytułu nieuprawnionych działań .....	17
4.2.5.5. Pracownicy kontraktowi .....	17
4.2.5.6. Dokumentacja dla Personelu pełniącego Role zaufane.....	17
<b>4.3. Bezpieczna eksploatacja .....</b>	<b>17</b>
4.3.1. Rejestrowanie zdarzeń .....	17
4.3.2. Tworzenie kopii zapasowych i odtwarzanie .....	18

4.3.3.	Archiwizacja zdarzeń .....	18
4.4.	Zakończenie działalności w zakresie Usługi RDE PP lub przekazanie zadań przez Poczta Polska 19	
<b>5.</b>	<b>Zabezpieczenia techniczne .....</b>	<b>20</b>
5.1.	Zabezpieczenia sprzętu komputerowego.....	20
5.2.	Cykl życia zabezpieczeń technicznych .....	20
5.3.	Zabezpieczenia sieci .....	21
5.4.	Usługa pieczęci elektronicznej .....	22
5.5.	Usługa znakowania czasem.....	23
5.6.	Zabezpieczenia kryptograficzne .....	23
<b>6.</b>	<b>Audyty zgodności i inne oceny .....</b>	<b>23</b>
6.1.	Częstotliwość i okoliczności oceny .....	24
6.2.	Tożsamość i kwalifikacje audytora .....	24
6.3.	Związek audytora z audytowaną jednostką .....	24
6.4.	Zagadnienia objęte audytem .....	24
6.5.	Działania podejmowane celem usunięcia usterek wykrytych podczas audytu.....	25
6.6.	Informowanie o wynikach audytu.....	25
<b>7.</b>	<b>Inne postanowienia .....</b>	<b>25</b>
7.1.	Opłaty.....	25
7.2.	Niedyskryminujące zastosowanie .....	25
7.3.	Odpowiedzialność finansowa .....	25
7.4.	Poufność informacji.....	25
7.5.	Ochrona danych osobowych .....	26
7.6.	Prawo do własności intelektualnej.....	26
7.7.	Zgodność z obowiązującym prawem .....	26
7.8.	Zobowiązania i gwarancje.....	26
7.8.1.	Zobowiązania Poczty Polskiej .....	26
7.8.2.	Zobowiązania zewnętrznych podmiotów .....	27

7.8.3.	Zobowiązania Klientów.....	27
<b>7.9.</b>	<b>Ograniczenia odpowiedzialności .....</b>	<b>27</b>
<b>7.10.</b>	<b>Odszkodowania.....</b>	<b>28</b>
<b>7.11.</b>	<b>Procedura wprowadzania zmian .....</b>	<b>28</b>

## 1. Wstęp

### 1.1. Wprowadzenie

Niniejsza Polityka świadczenia usługi i deklaracja praktyk dla usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A. („**Polityka**”) określa ogólne zasady stosowane przez Poczta Polską S.A. w trakcie świadczenia kwalifikowanej usługi rejestrowanego doręczenia elektronicznego. Polityka definiuje Strony Usługi RDE, określa ich obowiązki i odpowiedzialność oraz obszary zastosowań jej regulacji. Ponadto określa rozwiązania, w tym techniczne i organizacyjne, wskazujące warunki zabezpieczeń dla Usługi RDE.

### 1.2. Słownik

Użyte w Polityce określenia oznaczają:

- 1) **Dane identyfikujące osobę** – zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej osobę prawną;
- 2) **Dostawca usług zaufania** – dostawca usługi zaufania (np. kwalifikowanej usługi elektronicznego znacznika czasu lub usługi zaawansowanej pieczęci elektronicznej), będący osobą fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany dostawca usług zaufania;
- 3) **Dyrektor BAC** – Dyrektor Biura Analiz i Cyfryzacji Procesów;
- 4) **ETSI** – normy Europejskiego Instytutu Norm Telekomunikacyjnych:
  - a) ETSI EN 319 401 v3.2.1 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*,
  - b) ETSI EN 319 521 v1.1.1 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers*;
- 5) **HSM** (ang. Hardware Security Module) – sprzętowy moduł bezpieczeństwa, stanowiący w pełni zabezpieczone urządzenie do przechowywania i zarządzania kluczami bezpieczeństwa do krytycznej autoryzacji i przetwarzania kryptograficznego oraz zapewniający całe spektrum zastosowań: od szyfrowania danych cyfrowych w procesach i transakcjach biznesowych, poprzez zabezpieczenie dokumentów elektronicznych w urzędach i instytucjach, po zarządzanie kluczami dostępu i bezpieczeństwo w ramach wymiany danych;
- 6) **Konektor AS4** – interfejs do komunikacji za pomocą protokołu AS4 (warstwa transportowa, MSH), który jest odpowiedzialny za nawiązywanie połączenia pomiędzy Systemem RDE a systemem danej Usługi RDE oraz poprawność tego połączenia;
- 7) **Krajowy Schemat Identyfikacji** – krajowy schemat identyfikacji elektronicznej obejmujący:

- a) węzeł krajowy identyfikacji elektronicznej („węzeł krajowy”),
  - b) przyłączone do węzła krajowego:
    - systemy identyfikacji elektronicznej, w których wydawane są środki identyfikacji elektronicznej,
    - systemy teleinformatyczne, w których udostępniane są usługi online,
  - c) węzeł wykorzystywany w procesie transgranicznego uwierzytelniania osób, o którym mowa w przepisach wydanych na podstawie Rozporządzenia eIDAS („węzeł transgraniczny”);
- 8) **Kwalifikowana Usługa RDE (Usługa RDE PP)** – świadczona przez Poczta Polska kwalifikowana usługa rejestrowanego doręczenia elektronicznego, umożliwiająca przesłanie danych pomiędzy stronami trzecimi drogą elektroniczną i zapewniająca dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniąca przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiegokolwiek nieupoważnionej zmiany, spełniająca wymogi, o których mowa w art. 44 Rozporządzenia eIDAS;
- 9) **Kwalifikowany dostawca usług zaufania** – dostawca usług zaufania, któremu status kwalifikowany nadaje organ nadzoru;
- 10) **Personel** – osoby zatrudnione odpowiednio, przez Poczta Polska S.A. lub Poczta Polska Usługi Cyfrowe Sp. z o.o. na podstawie umowy o pracę oraz osoby fizyczne świadczące osobiście usługi na rzecz Poczty Polskiej S.A. lub Poczty Polskiej Usługi Cyfrowe Sp. z o.o. w oparciu o umowę cywilnoprawną (umowę o dzieło, umowę zlecenia, umowę o świadczenie usług), w tym członkowie Zarządu i Rady Nadzorczej Poczty Polskiej S.A. lub Poczty Polskiej Usługi Cyfrowe Sp. z o.o.;
- 11) **Poziom wiarygodności (bezpieczeństwa)** – poziom bezpieczeństwa identyfikacji elektronicznej zgodnie z art. 8 Rozporządzenia eIDAS, określanej niekiedy jako poziom zaufania lub wiarygodności (tłum. z j. ang. *Level of assurance*);
- 12) **Poczta Polska** – Poczta Polska S.A.;
- 13) **PPUC** – Poczta Polska Usługi Cyfrowe Sp. z o.o.;
- 14) **Przesyłka** – dane przesyłane pomiędzy stronami z wykorzystaniem Usługi RDE PP;
- 15) **Regulamin** – Regulamin świadczenia kwalifikowanej usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A., dostępny na stronie internetowej [www.bip.poczta-polska.pl/repozytorium/](http://www.bip.poczta-polska.pl/repozytorium/) oraz w każdej placówce Poczty Polskiej;
- 16) **Role zaufane** – role pełnione przez wyznaczonych członków Personelu w zakresie wskazanym w Podrozdziale 4.2.1. Polityki;
- 17) **Rozporządzenie eIDAS** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE z późn. zm.;
- 18) **Strony Usługi RDE PP** – podmioty wskazane w Podrozdziale 1.3. Polityki;

- 19) **System identyfikacji elektronicznej** – system identyfikacji elektronicznej, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym lub prawnym, lub osobom fizycznym reprezentującym osoby prawne;
- 20) **System RDE** – wszystkie elementy organizacyjne i techniczne, wymagające konfiguracji, zapewniające funkcjonowanie Usługi RDE PP;
- 21) **Środek identyfikacji elektronicznej** – materialna lub niematerialna jednostka zawierająca dane identyfikujące osobę i używana do celów uwierzytelniania dla usługi online;
- 22) **Usługa RDE** – kwalifikowana usługa rejestrowanego doręczenia elektronicznego, umożliwiająca przesłanie danych pomiędzy stronami trzecimi drogą elektroniczną i zapewniająca dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniąca przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiegokolwiek nieupoważnionej zmiany, spełniająca wymogi, o których mowa w art. 44 Rozporządzenia eIDAS, świadczona przez innego dostawcę niż Poczta Polska;
- 23) **Usługa zaufania** – świadczona za wynagrodzeniem usługa elektroniczna obejmująca czynności wskazane w art. 3 pkt 16 lit. A-c Rozporządzenia eIDAS;
- 24) **Ustawa** – ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

### 1.3. Definicje Stron Usługi RDE PP

Nazwa strony	Opis
Dostawca Usługi RDE PP	Poczta Polska będąca samodzielnym dostawcą Usługi RDE PP
Dostawca Usługi RDE	Dostawca kwalifikowanej usługi rejestrowanego doręczenia elektronicznego, inny niż Poczta Polska
Dostawca usługi identyfikacji elektronicznej	Dostawca środka identyfikacji elektronicznej w ramach notyfikowanego krajowego schematu identyfikacji elektronicznej zapewniający klientom usługi możliwość identyfikacji i uwierzytelnienia
Techniczny dostawca rozwiązania Usługi RDE PP	PPUC z siedzibą w Warszawie, funkcjonująca pod marką Envelo
Klient	Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, będąca nadawcą lub odbiorcą przesyłki elektronicznej

Strona ufająca	Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, polegająca na zaufaniu do usługi zaufania rejestrowanego doręczenia elektronicznego opisanego w Polityce
Inny dostawca usługi zaufania	Inny niż Poczta Polska dostawca usługi zaufania, (np. kwalifikowanej usługi elektronicznego znacznika czasu lub usługi zaawansowanej pieczęci elektronicznej)

#### **1.4. Zakres Usługi RDE PP**

1. Usługa RDE PP może być realizowana przez Poczta Polską, lub też może umożliwiać doręczenie korespondencji dzięki współpracy Poczty Polskiej z innymi Dostawcami Usług RDE.
2. Wszyscy Kwalifikowani dostawcy usług zaufania współpracujący z Poczta Polską są zobowiązani spełniać wymagania bezpieczeństwa wynikające z Polityki.

#### **1.5. Podstawowe elementy Usługi RDE PP**

1. Usługa RDE PP składa się z następujących elementów: wysłania Przesyłki, odbioru Przesyłki i wystawienia dowodów dokonanych czynności:
  - 1) wysłanie Przesyłki obejmujące następujące kroki:
    - a) identyfikację i uwierzytelnienie Klienta realizującego nadanie Przesyłki w Systemie RDE,
    - b) przekazanie przez Klienta Przesyłki do nadania przez dostawcę Usługi RDE PP,
    - c) wystawienie dowodu nadania przez dostawcę Usługi RDE PP;
  - 2) odbiór Przesyłki obejmujący następujące kroki:
    - a) w przypadku adresata obsługiwanego przez Dostawcę Usługi RDE PP:
      - przekazanie przez Dostawcę Usługi RDE PP do Klienta w roli odbiorcy informacji o nowej Przesyłce i prośba o akceptację przyjęcia Przesyłki,
      - akceptacja lub odmowa akceptacji przez Klienta Przesyłki, przy czym odmowa akceptacji Przesyłki może także zostać zrealizowana poprzez zaniechanie jej odbioru,
      - wystawienie dowodu preawizacji Przesyłki przez Dostawcę Usługi RDE PP,
      - identyfikacja i uwierzytelnienie przez System RDE Klienta przed odbiorem Przesyłki,
      - przekazanie Przesyłki poza Usługę RDE PP do odbiorcy,
    - b) w przypadku adresata obsługiwanego przez Dostawcę Usługi RDE innego niż Poczta Polska – przekazanie przesyłki do tego Dostawcy;
  - 3) wystawienie dowodów:
    - a) nadania Przesyłki (w tym dokładny czas nadania) – dostępny dla nadawcy Usługi RDE PP,

- b) preawizacji – dostępny dla nadawcy i odbiorcy,
  - c) przekazania Przesyłki pomiędzy Dostawcą Usługi RDE PP a Dostawcą Usługi RDE, z obowiązkiem przekazania dowodu wysłania,
  - d) odbioru Przesyłki (w tym dokładny czas odbioru) – dostępny dla nadawcy i odbiorcy (generowany także w przypadku zaniechania odbioru).
2. Przesyłka, przekazana do Poczty Polskiej, zaadresowana do więcej niż jednego adresata nie zostanie przyjęta przez Pocztę Polską.
  3. Przesyłki w Usłudze RDE obsługiwane są w trybie zgody określonym w standardzie [ETSI3195222].
  4. Przesyłka, przekazana do Poczty Polskiej w trybie innym niż zgoda adresata nie zostanie przyjęta przez Pocztę Polską.
  5. Każda zmiana danych niezbędna do celów wysłania lub otrzymania danych jest wyraźnie wskazana nadawcy (przed wysłaniem) i adresatowi (przed odbiorem) danych w postaci komunikatu elektronicznego.
  6. Informacje o przesyłce w wystawianych przez Dostawcę Usługi RDE PP dowodach są tworzone z wykorzystaniem funkcji skrótu SHA3-512.
  7. Przekazywane do Dostawcy Usługi RDE PP, wystawione przez Dostawcę Usługi RDE, dowody zawierające informacje o Przesyłce, wykorzystujące funkcję skrótu inną niż SHA3-512, nie będą przyjmowane przez dostawcę Usługi RDE PP.
  8. Dowody w zakresie nadania, preawizacji, przekazania oraz odbioru Przesyłki są zabezpieczone pieczęcią elektroniczną oraz znakowane czasem. Poczta Polska udostępnia Klientom dowody wytworzone w procesie świadczenia Usługi RDE PP przez okres nie krótszy niż 24 miesiące od momentu ich wytworzenia.
  9. Niezależnie od utraty danych z powodów technicznych lub innych, Poczta Polska zapewnia utrzymanie dokumentów i danych, wynikających z art. 17 Ustawy, przez okres 20 lat od momentu ich wytworzenia.

## **2. Administracja i repozytorium**

### **2.1. Administracja Polityką**

1. Poczta Polska wskazuje Dyrektora BAC, jako podmiot odpowiedzialny za administrowanie Polityką.
2. Każdorazowa zmiana Polityki wymaga podjęcia uchwały przez Zarząd Poczty Polskiej. Z chwilą dokonania zmian, w Metryce dokumentu wskazywany jest aktualny status danej wersji Polityki i data, od której obowiązuje.
3. Za ocenę aktualności i przydatności Polityki odpowiada Dyrektor BAC.
4. W ramach świadczenia Usługi RDE PP, Poczta Polska dokonuje przeglądów stosowanych praktyk zgodnie z prowadzoną procedurą zarządzania ryzykiem.

### **2.2. Repozytorium i publikacja dokumentu**

1. Repozytorium jest centralną bazą danych zawierającą informacje o:

- 1) aktualnej i obowiązującej wersji Polityki;
  - 2) historycznych wersjach Polityki;
  - 3) regulaminie Usługi RDE PP;
  - 4) innych dokumentach przeznaczonych do publikacji na podstawie Polityki, jeśli takie wskazano.
2. Dokumenty umieszczone w repozytorium są publicznie dostępne pod adresem <https://bip.poczta-polska.pl/repozytorium/>.
  3. Wszelkie zmiany Polityki są archiwizowane, a ich zmienione wersje publikowane na bieżąco (każdorazowo, gdy zostaną uaktualnione lub zmienione).
  4. Wszystkie informacje publikowane w repozytorium są ogólnie dostępne. Informacje te są zabezpieczone przed nieautoryzowanym zmienianiem, dodawaniem i usuwaniem oraz są przechowywane z zachowaniem kopii zapasowych.

### **3. Identyfikacja i uwierzytelnienie**

1. Poczta Polska w ramach Usługi RDE PP korzysta z zewnętrznego procesu identyfikacji elektronicznej, w ramach Usługi RDE PP nie jest wydawany środek uwierzytelniający.
2. Każdy adres do doręczeń elektronicznych zapewnia jednoznaczną identyfikację nadawcy i odbiorcy. Usługa RDE PP dopuszcza równoległe funkcjonowanie podstawowego adresu wraz z adresami funkcjonującymi u innych dostawców Usługi RDE. W zakresie adresacji Usługa RDE PP umożliwia korzystanie ze wspólnej infrastruktury adresowej udostępnionej przez ministra właściwego ds. informatyzacji na podstawie właściwych przepisów.
3. Usługa RDE PP umożliwia mapowanie adresu do doręczeń elektronicznych, w szczególności w zakresie akceptacji wiadomości pochodzących od innych Dostawców Usług RDE, a także wiadomości doręczanych w ramach krajowych ram dla doręczeń.
4. W ramach Usługi RDE PP dopuszcza się następujące sposoby identyfikacji i uwierzytelnienia:
  - 1) w oparciu o Krajowy Schemat Identyfikacji zgodnie z art. 21a Ustawy, w szczególności Środki identyfikacji elektronicznej wchodzące w skład Krajowego Schematu Identyfikacji pozwalające na założenie Profilu Zaufanego („eGO”);
  - 2) w oparciu o zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną na podstawie certyfikatów rozpoznawanych przez Usługę RDE tzn. certyfikat kwalifikowany, certyfikat podpisu osobistego oraz inne certyfikaty wydane na podstawie polityki certyfikacji zgodnej z profilem NCP+ określonym standardem ETSI EN 319411-2;
  - 3) w oparciu o środek identyfikacji elektronicznej uznany na poziomie krajowym, w szczególności środek stosowany do uwierzytelniania w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy, spełniającym warunki ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

5. Identyfikacja elektroniczna przeprowadzana jest za każdym razem przed nadaniem lub doręczeniem Przesyłki. Jeżeli identyfikacja odbiorcy opiera się na zaawansowanym podpisie elektronicznym, weryfikacja podpisu poprzedza przekazanie Przesyłki.
6. Poczta Polska, wykorzystując do identyfikacji elektronicznej zewnętrzne systemy identyfikacji elektronicznej, zapewnia, że systemy te są uznane krajowo oraz oferują identyfikację bezpieczeństwa na średnim poziomie wiarygodności.

#### **4. Zabezpieczenia organizacyjne, operacyjne i fizyczne**

1. Poczta Polska posiada wewnętrzny dokument dotyczący polityki bezpieczeństwa informacji, który określa podstawowe zasady zarządzania bezpieczeństwem informacji w zakresie Usługi RDE PP.
2. Wewnętrzny dokument dotyczący polityki bezpieczeństwa informacji jest komunikowany każdej osobie pełniącej Rolę zaufaną w zakresie Usługi RDE PP, zaś Poczta Polska jest zobowiązana do dokumentowania oświadczeń tych osób o zobowiązaniu się do przestrzegania zasad i wytycznych ujętych w ww. dokumencie.

##### **4.1. Zabezpieczenia fizyczne**

###### **4.1.1. Lokalizacja i budynki**

Systemy teleinformatyczne wykorzystywane do świadczenia Usługi RDE PP mieszczą się w dwóch niezależnych lokalizacjach (centrum podstawowym i centrum zapasowym).

###### **4.1.2. Dostęp fizyczny**

1. Fizyczny dostęp do budynku oraz pomieszczeń wykorzystywanych w ramach świadczenia Usługi RDE PP jest kontrolowany przez pracowników ochrony oraz nadzorowany przez elektroniczny system zabezpieczenia technicznego.
2. Ochrona fizyczna budynków funkcjonuje 24 godziny na dobę.
3. Pomieszczenia, w których znajduje się system teleinformatyczny, w tym także pomieszczenia, w których znajduje się bezpieczny moduł kryptograficzny, wyposażone są w system kontroli dostępu do pomieszczeń oraz system sygnalizacji włamania i napadu.
4. Dostęp do pomieszczeń wykorzystywanych w ramach świadczenia Usługi RDE PP posiadają tylko osoby upoważnione.
5. Weryfikacja uprawnień dostępu do pomieszczeń realizowana jest w oparciu o elektroniczny system kontroli dostępu umożliwiającą identyfikację i rozliczalność osób upoważnionych.

###### **4.1.3. Bezpieczeństwo środowiskowe**

1. W przypadku zaniku zasilania podstawowego System RDE przechodzi na zasilanie awaryjne poprzez UPS, czyli urządzenie, którego funkcją jest nieprzerwane zasilanie urządzeń elektronicznych Systemu RDE.

2. Środowisko pracy w pomieszczeniach systemu komputerowego kontrolowane jest w sposób ciągły i niezależny od innych pomieszczeń. Ponadto wszystkie pomieszczenia są klimatyzowane.
3. Czujniki zalania są zainstalowane w pomieszczeniach serwerowni. Alarmy o zalaniu przekazywane są do ochrony i administratora budynku, którzy zawiadamiają odpowiednie służby miejskie, Inspektora bezpieczeństwa oraz Administratora systemu.
4. System ochrony przeciwpożarowej, zainstalowany w pomieszczeniach systemu komputerowego, spełnia wymogi stosownych przepisów i norm przeciwpożarowych. W serwerowni zainstalowane są urządzenia gaśnicze (gazowe), które załączają się automatycznie, w przypadku wykrycia pożaru w chronionym obszarze.

#### **4.1.4. Nośniki informacji**

Nośniki, na których przechowywane są kopie bezpieczeństwa środowiska kryptograficznego, składowane są w sejfach ogniodpornych. Dostęp do sejfów mają osoby pełniące role Inspektora bezpieczeństwa, Administratora systemu oraz Audytora.

#### **4.1.5. Niszczenie informacji**

Papierowe oraz elektroniczne nośniki zawierające informacje, mogące mieć wpływ na bezpieczeństwo Poczty Polskiej, dane osobowe oraz informacje stanowiące tajemnicę pocztową, po upływie okresu przechowywania rejestrowanych i archiwizowanych zdarzeń niszczone są w urządzeniach specjalnie do tego przeznaczonych.

#### **4.1.6. Kopie bezpieczeństwa**

1. Zapisy zdarzeń są kopiowane zgodnie z harmonogramem tworzenia kopii bezpieczeństwa systemu teleinformatycznego. Kopie te przechowywane są w sejfach znajdujących się w centrum podstawowym.
2. Czynności tworzenia kopii zapasowych wykonywane są przez Operatora systemu w obecności Inspektora bezpieczeństwa.

### **4.2. Zabezpieczenia organizacyjne**

#### **4.2.1. Role zaufane**

1. Osoby sprawujące nadzór nad Systemem RDE pełnią określone Role zaufane, które zaprezentowano w poniższej tabeli.

Nazwa Roli zaufanej	Zakres głównych obowiązków
Dyrektor BAC	<ul style="list-style-type: none"> <li>▪ Zapewnienie prawidłowej organizacji i funkcjonowania Usługi RDE PP. Wdrożenie/Wdrażanie postanowień Polityki.</li> <li>▪ Zapewnienie zgodności Usługi RDE PP z prawem oraz standardami normalizacyjnymi.</li> <li>▪ Nadzorowanie zapewnienia ciągłości działania oraz zapewnienie realizacji planu zakończenia działalności.</li> </ul>

Kierownik Działu odpowiedzialny za systemy usług zaufania	<ul style="list-style-type: none"> <li>▪ Zarządzanie działem i nadzorowanie jego funkcjonowania.</li> <li>▪ Zapewnienie prawidłowej organizacji i funkcjonowania Systemu RDE.</li> <li>▪ Realizacja kierunków rozwoju usług.</li> <li>▪ Utrzymanie aktualności planu zakończenia działalności.</li> </ul>
Operator systemu	<ul style="list-style-type: none"> <li>▪ Instalowanie, konfigurowanie i zarządzanie systemami oraz sieciami teleinformatycznymi wykorzystywanymi na potrzeby świadczenia Usługi RDE PP.</li> <li>▪ Dbałość o operacyjne aspekty świadczenia Usługi RDE PP.</li> <li>▪ Wykonywanie procedur i instrukcji operacyjnych.</li> <li>▪ Realizacja procedur utrzymania Systemu RDE.</li> </ul>
Administrator systemu	<ul style="list-style-type: none"> <li>▪ Zapewnienie współpracy z dostawcą (dostawcami), w szczególności z PPUC i umiejscowionymi u tego dostawcy Operatorami systemu.</li> <li>▪ Operacyjne czynności w zakresie zarządzania kluczami.</li> </ul>
Inspektor bezpieczeństwa	<ul style="list-style-type: none"> <li>▪ Zapewnienie bezpieczeństwa procesu w ramach świadczonej Usługi RDE PP.</li> <li>▪ Wdrażanie i realizacja postanowień wewnętrznego dokumentu dotyczącego polityki bezpieczeństwa informacji, w tym m.in.: <ul style="list-style-type: none"> <li>✓ zapewnienie zarządzania ryzykiem,</li> <li>✓ nadzorowanie procesu zarządzania incydentami,</li> <li>✓ nadzorowanie bezpieczeństwa fizycznego, bezpieczeństwa sieci oraz zarządzania ciągłością działania,</li> <li>✓ zarządzanie uprawnieniami w zakresie Usługi RDE PP.</li> </ul> </li> </ul>
Audytor	<ul style="list-style-type: none"> <li>▪ Przeglądanie archiwów i dzienników zdarzeń Usługi RDE PP.</li> <li>▪ Analizowanie zdarzeń i incydentów dotyczących Usługi RDE PP.</li> <li>▪ Rekomendowanie działań naprawczych i profilaktycznych.</li> <li>▪ Kontrola wdrożonych mechanizmów i środków bezpieczeństwa.</li> </ul>
Koordynator ds. wdrożenia eUsług	<ul style="list-style-type: none"> <li>▪ Koordynowanie działań dotyczących Usługi RDE PP.</li> </ul>
Inspektor ds. weryfikowania tożsamości	<ul style="list-style-type: none"> <li>▪ Odpowiedzialność za proces weryfikacji tożsamości nadawcy i odbiorcy i zgodność jego rzeczywistego przebiegu z przyjętymi założeniami.</li> </ul>

2. Wymienione w ust. 1 role i obowiązki związane z bezpieczeństwem (Inspektor bezpieczeństwa oraz Audytor) zostały również szczegółowo określone w wewnętrznym dokumencie dotyczącym polityki bezpieczeństwa informacji.
3. Poczta Polska deklaruje, że opisany zakres obowiązków dokumentuje się w opisie danego stanowiska, jak również w wewnętrznym dokumencie opisującym szczegółowo zakres odpowiedzialności dla poszczególnej Roli zaufanej w Systemie RDE.
4. Bezpośredni udział w procesie administrowania danymi osobowymi mają osoby w Roli zaufanej, które zostały zweryfikowane, w szczególności z uwzględnieniem wymagań wynikających z norm ETSI.

#### **4.2.2. Role zaufane podlegające separacji obowiązków**

1. Role zaufane wyodrębnione w ramach Personelu zapobiegają nadużyciom, przy korzystaniu z Systemu RDE.
2. Każdej osobie odpowiedzialnej za eksploatację Systemu RDE wykorzystywanego do świadczenia Usługi RDE PP przydzielono tylko takie prawa, które wynikają z pełnionej przez nią Roli zaufanej i ponoszonej z tego tytułu odpowiedzialności.
3. Rola Inspektora bezpieczeństwa nie może być łączona z rolą Administratora systemu ani z rolą Operatora systemu. Rola Audytora nie może być łączona z żadną z pozostałych Ról zaufanych.

#### **4.2.3. Zarządzanie incydentami**

1. Poczta Polska na żądanie ministra właściwego ds. informatyzacji, z zachowaniem przepisów o ochronie informacji prawnie chronionych, udziela informacji lub udostępnia dokumenty, które są bezpośrednio związane ze świadczonymi Usługami zaufania lub mają wpływ na świadczone Usługi zaufania, w tym dotyczą zarządzania incydentami związanymi z Usługą RDE PP.
2. Poczta Polska bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu incydentu, zawiadamia ministra właściwego ds. informatyzacji, w stosownych przypadkach, inne właściwe podmioty, o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną Usługę zaufania lub przetwarzane w jej ramach dane osobowe.
3. Powyższe obowiązki notyfikacyjne pozostają bez uszczerbku dla obowiązków notyfikacyjnych Poczty Polskiej wynikających z odrębnych przepisów, w tym w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
4. W ramach świadczenia Usługi RDE PP istnieje także procedura wewnętrzna regulująca zarządzanie incydentami.

#### **4.2.4. Zarządzanie ryzykiem**

Zarządzanie ryzykiem prowadzone jest zgodnie z ustanowioną w Poczcie Polskiej procedurą zarządzania ryzykiem, w celu dostosowania zabezpieczeń techniczno-organizacyjnych do zidentyfikowanych zagrożeń dla Usługi RDE PP.

#### **4.2.5. Nadzór nad Personelem pełniącym Role zaufane**

##### **4.2.5.1. Kwalifikacje, doświadczenie, upoważnienia**

Osoby uczestniczące w świadczeniu Usługi RDE PP, pełniące Role zaufane, posiadają odpowiednie kwalifikacje przewidziane dla Kwalifikowanych dostawców usług zaufania, w szczególności wiedzę

i umiejętności z zakresu infrastruktury klucza publicznego oraz przetwarzania danych osobowych, a ponadto:

- 1) posiadają pełną zdolność do czynności prawnych;
- 2) posiadają minimum wykształcenie średnie;
- 3) zobowiązały się do nieujawniania informacji wrażliwych, z punktu widzenia bezpieczeństwa dostawcy Usługi RDE PP lub poufności danych Klienta, wynikających z wewnętrznego dokumentu dotyczącego polityki bezpieczeństwa informacji;
- 4) nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem znacznika czasu a działającymi w jego imieniu punktami rejestracji;
- 5) zapoznały się z wewnętrznymi procedurami Poczty Polskiej dotyczącymi Usługi RDE PP,
- 6) zostały poinformowane o odpowiedzialności karnej w zakresie związanym ze świadczeniem Usług zaufania;
- 7) zostały przeszkolone w zakresie zasad świadczenia Usług zaufania, w tym: wdrożonych procedur i polityk oraz związanych z nimi zasad bezpieczeństwa.

#### **4.2.5.2. Weryfikacja Personelu**

1. Przed powierzeniem Personelowi którejkolwiek z Ról zaufanych przeprowadzana jest co najmniej weryfikacja:
  - 1) świadectwa pracy z poprzednich miejsc zatrudnienia (w przypadku nowej osoby);
  - 2) dyplomu i świadectwa potwierdzających wykształcenie tej osoby;
  - 3) kwalifikacji i doświadczenia zawodowego.
2. Weryfikacja przeprowadzana jest z poszanowaniem wymogów określonych we właściwych przepisach w zakresie przetwarzania danych osobowych.

#### **4.2.5.3. Szkolenia**

1. Osoby pełniące Role zaufane w ramach Usługi RDE PP przechodzą cykl szkoleń dotyczących:
  - 1) zasad określonych w Polityce;
  - 2) zasad zawartych w dokumentacji przypisanej Roli zaufanej, którą dana osoba pełni i zakresu obowiązków, które będzie wykonywała;
  - 3) ochrony danych osobowych i ochrony informacji;
  - 4) infrastruktury klucza publicznego;
  - 5) zasad i mechanizmów zabezpieczeń stosowanych w Usłudze RDE PP;
  - 6) oprogramowania systemu komputerowego Usługi RDE PP;
  - 7) procedur realizowanych po awariach lub katastrofach Systemu RDE;
  - 8) zagrożeń i aktualnych praktyk bezpieczeństwa.
2. Szkolenia, o których mowa w ust. 1, są powtarzane co najmniej raz na dwa lata oraz w zależności od potrzeb zawsze wtedy, gdy nastąpiły istotne zmiany w świadczeniu Usługi RDE PP.

#### **4.2.5.4. Sankcje z tytułu nieuprawnionych działań**

1. W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie ze strony Personelu, Administrator systemu w porozumieniu z Inspektorem bezpieczeństwa może w pierwszej kolejności zablokować dostęp do Systemu RDE sprawcy takiego zdarzenia.
2. Dalsze postępowanie przeprowadzane jest w porozumieniu z Zarządem Poczty Polskiej i może prowadzić do złożenia zawiadomienia o możliwości popełnienia przestępstwa.
3. Osoby pełniące Role zaufane oraz wszyscy zewnątrzni dostawcy zostali poinformowani o sankcjach karnych wynikających z Ustawy.

#### **4.2.5.5. Pracownicy kontraktowi**

1. Dopuszcza się zatrudnianie pracowników kontraktowych, w celu zapewnienia niezbędnych zasobów w kontekście świadczenia Usługi RDE PP.
2. Zakres odpowiedzialności osób fizycznych świadczących osobiście usługi na rzecz Poczty Polskiej lub PPUC w oparciu o umowę cywilnoprawną (umowę o dzieło, umowę zlecenia, umowę o świadczenie usług) został zdefiniowany w stosownych umowach dotyczących współpracy.

#### **4.2.5.6. Dokumentacja dla Personelu pełniącego Role zaufane**

Poczta Polska umożliwi członkom swojego Personelu pełniącym Role zaufane dostęp do następujących dokumentów:

- 1) Polityki;
- 2) procedur eksploatacyjnych (tylko dla Ról zaufanych) w zakresie obsługi Systemu RDE;
- 3) stosowanych formularzy wniosków;
- 4) niezbędnych wyciągów z dokumentacji (właściwej dla pełnionej Roli zaufanej), w tym procedur awaryjnych;
- 5) zakresu obowiązków i uprawnień wynikających z pełnionej Roli zaufanej.

### **4.3. Bezpieczna eksploatacja**

#### **4.3.1. Rejestrowanie zdarzeń**

1. W ramach Usługi RDE PP rejestrowaniu podlegają w szczególności następujące zdarzenia:
  - 1) zdarzenia bezpośrednio związane ze świadczeniem Usług zaufania, a w szczególności:
    - a) dowody na to, że zasady i warunki świadczenia Usługi RDE PP zostały zaakceptowane przez Klienta,
    - b) czynności systemowe dotyczące dostępu do systemów informatycznych, korzystania z systemów informatycznych i zgłoszeń serwisowych,
    - c) czynności związane z identyfikacją i uwierzytelnieniem Klientów Usługi RDE PP,
    - d) czynności związane z obsługą Klientów, w tym dowody w zakresie m.in. wysłania i odbioru Przesyłek;
  - 2) logi systemowe z serwerów i stacji roboczych wchodzących w skład Systemu RDE;

- 3) zdarzenia związane z obsługą techniczną systemu, tj.: błędy i alarmy, rejestr wprowadzanych zmian w systemie;
  - 4) zdarzenia związane z bezpieczeństwem, w tym zmiany związane z wewnętrznym dokumentem dotyczącym polityki bezpieczeństwa informacji, uruchamianiem i zamykaniem Systemu RDE, awariami Systemu RDE i awariami sprzętu, działaniami zapory i routera oraz próbami dostępu do Systemu RDE.
2. Poczta Polska zapewnia przechowywanie dowodów w postaci raportów z prowadzonych testów bezpieczeństwa, audytów konfiguracji oraz testów penetracyjnych.
  3. Logi są zabezpieczone przed modyfikacją, podlegają procedurom tworzenia kopii zapasowych oraz są archiwizowane.
  4. Dostęp do archiwów mają: Audytor, Dyrektor BAC oraz osoby upoważnione przez Dyrektora BAC.
  5. Rejestry zdarzeń zapisywane są w formie elektronicznej. Rekordy zawierają: identyfikator zdarzenia, datę i czas wystąpienia zdarzenia, typ i szczegółowy opis zdarzenia. Stary rejestr po zarchiwizowaniu jest usuwany z dysku, zgodnie z wewnętrzną polityką archiwizacji.
  6. Zapisy rejestrowanych zdarzeń przechowywane są w plikach na dysku systemowym, przez okres przynajmniej 24 miesięcy.
  7. Czas wykorzystywany do rejestrowania zdarzeń zgodnie z wymaganiami w rejestrze zdarzeń jest synchronizowany z UTC, co najmniej raz dziennie.

#### **4.3.2. Tworzenie kopii zapasowych i odtwarzanie**

1. Kopie zapasowe wykonywane są automatycznie zgodnie z harmonogramem tworzenia kopii bezpieczeństwa Systemu RDE, który jest weryfikowany zgodnie z wewnętrznymi procedurami Poczty Polskiej.
2. Kopie zapasowe przechowywane są w bezpiecznej lokalizacji niezależnej od centrum podstawowego.

#### **4.3.3. Archiwizacja zdarzeń**

1. W ramach Usługi RDE PP archiwizacji podlegają w szczególności:
  - 1) dane identyfikacyjne Klientów lub Personelu pełniącego Role zaufane;
  - 2) dane uwierzytelniające Klientów lub Personelu pełniącego Role zaufane;
  - 3) dowód, że tożsamość nadawcy została pierwotnie zweryfikowana;
  - 4) logi operacji Usługi RDE PP, weryfikacji tożsamości nadawcy i odbiorcy oraz komunikacji;
  - 5) dowody weryfikacji tożsamości odbiorcy przed wysyłką/przekazaniem Przesyłki,
  - 6) dowody na to, że Przesyłka nie została zmodyfikowana podczas transmisji;
  - 7) odniesienie do lub przestanie całej Przesyłki;
  - 8) tokeny znaczników czasu odpowiadające dacie i godzinie wysyłania, przekazywania oraz modyfikowania Przesyłki, stosownie do przypadku;
  - 9) Polityka oraz jej historyczne wersje;

- 10) inne dokumenty umieszczone w repozytorium zgodnie z zapisami Polityki.
2. Archiwum zawiera również wszelkie dokumenty papierowe, związane ze świadczeniem Usługi RDE PP, których okres przechowywania wynosi 20 lat zgodnie z art. 17 Ustawy, z zastrzeżeniem art. 20 ust. 1 Ustawy.
3. Poczta Polska zapewnia poufność, integralność i dostępność tworzonych rejestrów zdarzeń.
4. Zapisy dotyczące funkcjonowania Usługi RDE PP są udostępniane, jeśli jest to wymagane, w celu udokumentowania prawidłowego działania Usługi RDE PP dla celów postępowania sądowego.

#### **4.4. Zakończenie działalności w zakresie Usługi RDE PP lub przekazanie zadań przez Poczta Polską**

1. Poczta Polska, mając na uwadze redukcję wpływu skutków podjęcia potencjalnej decyzji o zakończeniu świadczenia działalności w zakresie świadczenia Usługi RDE PP, planuje w szczególności spełnienie obowiązku odpowiednio wczesnego poinformowania o tym organu nadzoru, wszystkich Stron Usługi RDE PP, kontrahentów i partnerów, z którymi Poczta Polska jest związana umowami, na których zakończenie świadczenia Usługi RDE PP będzie miało wpływ, oraz przekazania dokumentów i danych związanych ze świadczeniem Usług zaufania organowi nadzoru.
2. Szczegółowy sposób postępowania w przypadku zakończenia działalności w zakresie świadczenia Usługi RDE PP określa Plan zakończenia działalności usługi rejestrowanego doręczenia elektronicznego w Poczcie Polskiej S.A.
3. Organ nadzoru jest informowany o planie zakończenia działalności w zakresie świadczenia Usługi RDE PP oraz każdorazowo o każdej jego zmianie.
4. Poczta Polska zobowiązuje się do wykonania następujących czynności:
  - 1) zapewnienia ciągłości pełnienia roli dostawcy Usługi RDE PP, nie dłużej niż 3 miesiące od dnia poinformowania organu nadzoru o zamiarze zaprzestania bądź niemożności pełnienia roli podmiotu dostawcy Usługi RDE PP;
  - 2) utrzymania dokumentów i danych wynikających z treści Polityki oraz danych wymaganych do weryfikacji poprawności świadczenia Usług zaufania, w tym dokumentów i danych przez okres 20 lat od ich wytworzenia;
  - 3) unieważnienia wszystkich wydanych pełnomocnictw do podpisywania umów o świadczenie Usługi RDE PP w imieniu Poczty Polskiej, nie później niż na dzień zakończenia działalności w zakresie świadczenia Usługi RDE PP;
  - 4) przekazania do zniszczenia lub wycofania kluczy urzędu Usług zaufania i ich kopii zapasowych, w przypadku, gdy nie przewiduje się dalszego wykorzystania tych danych lub w przypadku unieważnienia certyfikatu Dostawcy usług zaufania powiązanego z tymi usługami.

## **5. Zabezpieczenia techniczne**

1. Dane przesyłane pomiędzy stacjami roboczymi a serwerami muszą być szyfrowane, zaś zabezpieczenia Systemu RDE muszą spełniać wymogi aktów normatywnych obowiązujących w chwili świadczenia Usługi RDE PP.
2. Dane muszą być zabezpieczone przed utratą, modyfikacją, utratą integralności i nieuprawnionym dostępem.

### **5.1. Zabezpieczenia sprzętu komputerowego**

1. Wymagania techniczne określone w niniejszym rozdziale odnoszą się do kontroli zabezpieczeń pojedynczego komputera oraz zainstalowanego na nim oprogramowania w ramach Systemu RDE.
2. Funkcje zabezpieczające systemów komputerowych są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.
3. Pracownik, który pełni Rolę zaufaną, zobowiązany jest do blokowania swojej stacji roboczej zawsze, jeśli pozostaje ona poza jego nadzorem.
4. Komputery pracujące w Systemie RDE wyposażone są w następujące funkcje zabezpieczające:
  - 1) obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji (w przypadkach, gdy jest to istotne, np. z punktu widzenia pełnionej Roli zaufanej);
  - 2) uznaniową kontrolę dostępu;
  - 3) możliwość prowadzenia audytu zabezpieczeń;
  - 4) udostępnianie tylko osobom pełniącym Role zaufane;
  - 5) wymuszanie separacji obowiązków wynikających z pełnionych Ról zaufanych;
  - 6) wymuszanie wylogowania Personelu pełniącego Role zaufane po okresie bezczynności;
  - 7) identyfikację i uwierzytelnienie Ról zaufanych oraz pełniących je osób;
  - 8) kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenie baz danych;
  - 9) archiwizowanie danych dla potrzeb audytu;
  - 10) bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie Ról zaufanych oraz pełniących je osób;
  - 11) mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji;
  - 12) mechanizm monitorowania i alarmowania w przypadku wystąpienia zdarzeń nieautoryzowanego dostępu do zasobów komputera.

### **5.2. Cykl życia zabezpieczeń technicznych**

1. Nadzór nad wprowadzaniem modyfikacji lub zmian w Systemie RDE sprawuje Inspektor bezpieczeństwa. Zatwierdza on konfigurację Systemu RDE oraz wszelkie zmiany oprogramowania i sprzętu.

2. Testy nowych wersji oprogramowania lub wykorzystanie do tego celu istniejących baz danych odbywa się w środowisku testowym. Zasady stosowane przez Poczta Polską podczas przeprowadzania tych testów gwarantują nieprzerwaną pracę Systemu RDE, integralność jego zasobów oraz zachowanie poufności danych.
3. Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania Systemu RDE, które daje pewność, że system ten pracuje prawidłowo i jego funkcje są zgodne z zaplanowaną i zrealizowaną konfiguracją.
4. Mimo że prace administracyjne oraz zmiany w Systemie RDE są rejestrowane, to każda z wprowadzonych zmian wymaga dodatkowo zweryfikowania i akceptacji przez przynajmniej dwie osoby: Inspektora bezpieczeństwa oraz Administratora systemu.
5. System kontroli zmiany informuje uprawnionych pracowników o wystąpieniu modyfikacji w Systemie RDE i wymaga jej weryfikacji przez osobę inną od tej, która wprowadzała daną zmianę.
6. Aktualna konfiguracja Systemu RDE, jak również modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Zastosowane w Systemie RDE mechanizmy pozwalają na ciągłą weryfikację integralności oprogramowania, kontrolę ich wersji, a także uwierzytelnianie i weryfikowanie źródła pochodzenia.
7. Polityka nie narzuca cyklu życia stosowanych zabezpieczeń. Zabezpieczenia są wymieniane w przypadku zaistnienia potrzeby zastosowania innych niż obecnie używane, zmian w regulacjach prawnych lub jeśli są technologicznie przestarzałe i nie odpowiadają bieżącym normom i standardom.

### **5.3. Zabezpieczenia sieci**

1. Nadzór nad bezpieczeństwem sieci Systemu RDE sprawują Administratorzy systemu.
2. Sieć w ramach Usługi RDE PP podzielono na kilka logicznie odseparowanych segmentów, tj.:
  - 1) strefę chronioną serwerów, w tym serwerów aplikacji, baz danych, logów;
  - 2) strefę chronioną stacji Operatorów systemu;
  - 3) strefę chronioną stacji Administratorów systemu;
  - 4) strefę chronioną stacji Audytorów;
  - 5) strefę ograniczonego zaufania z publicznymi serwerami usługowymi.
3. Dla stref, o których mowa w ust. 2, stosuje się zdefiniowane polityki kontroli ruchu sieciowego.
4. Komunikacja ze strefy chronionej do stref publicznych jest zabezpieczona za pomocą skonfigurowanych narzędzi firewall. Dostęp od strony Internetu do każdego z segmentów chroniony jest przy pomocy narzędzi firewall.
5. Cała komunikacja pomiędzy systemami Usługi RDE PP, zlokalizowanymi w różnych ośrodkach, jest realizowana za pomocą szyfrowanych kanałów, zapewniających identyfikację Stron Usługi RDE PP oraz zabezpieczenie przed jakąkolwiek ingerencją w treść komunikacji.

6. W usłudze sieciowej wykorzystywane są najnowocześniejsze protokoły i algorytmy do szyfrowania na poziomie warstwy transportowej. Usługi sieciowe korzystają z certyfikatów uwierzytelniania strony internetowej TLS, jeśli dane są wysyłane poza sieciami wewnętrznymi. W szczególności dostęp użytkownika jest realizowany w protokole HTTPS.
7. Szczegółowy zakres połączeń pomiędzy poszczególnymi strefami jest opisany w dokumentacji Systemu RDE i stanowi tajemnicę przedsiębiorstwa Poczta Polska.
8. Na podstawie prowadzonych przeglądów konfiguracji sieci, przeglądów uprawnień kont sieciowych, jak również na podstawie wykonywanych analiz i testów bezpieczeństwa, wszelkie usługi sieciowe oraz konta sieciowe, które nie są używane, są blokowane lub dezaktywowane.
9. Poczta Polska przeprowadza regularnie (nie rzadziej niż raz na kwartał) skany podatności sieci. Ponadto, zapewnia, że wszelkie działania korygujące wobec zidentyfikowanych luk w zabezpieczeniach są rejestrowane.
10. W przypadku potrzeby zapewnienia wysokiego poziomu dostępności do Usługi RDE PP, zewnętrzne połączenia sieciowe będą nadmiarowe (redundantne), w przypadku pojedynczej awarii. Decyzje o podjęciu określonych środków bezpieczeństwa podejmowane są na mocy prowadzonych analiz ryzyka, zgodnie z wewnętrzną procedurą. Usługa RDE PP, łącząc się z dostawcami Usługi RDE oraz systemami zewnętrznymi, zapewnia ich identyfikację w oparciu o mechanizmy sieciowe, tj.: SSL lub IP-SEC.
11. Wszelkie zmiany wprowadzane w urządzeniach sieciowych wymagają wcześniejszej akceptacji Inspektora bezpieczeństwa. Przeprowadzona zmiana zostaje zaimplementowana dopiero po zweryfikowaniu jej przez Administratora systemu, który nie brał bezpośredniego udziału w przygotowywaniu zmiany. W przypadku znaczących zmian w konfiguracji Systemu RDE (po konfiguracji i po aktualizacji lub modyfikacjach infrastruktury lub aplikacji), Poczta Polska zapewnia przeprowadzenie testów penetracyjnych oraz gromadzi dowody z prowadzonych testów.
12. Jeśli nie wystąpiły inne okoliczności wymagające przeprowadzenia testu penetracyjnego, zostaje on przeprowadzony co najmniej raz na rok.

#### **5.4. Usługa pieczęci elektronicznej**

1. Wszystkie Przesyłki są zabezpieczone za pomocą usługi zaawansowanej pieczęci elektronicznej. Integralność Przesyłki i związanych z nią metadanych jest chroniona podczas transmisji, w szczególności w przypadku wymiany z nadawcą/odbiorcą lub między rozproszonymi komponentami Systemu RDE, a także w pamięci masowej. Ochrona integralności jest realizowana poprzez weryfikację pieczęci elektronicznych dla dokumentów nadawanych i odbieranych przez porównanie treści pieczęci.
2. Usługa zaawansowanej pieczęci elektronicznej jest obsługiwana w oparciu o certyfikaty wydane przez Narodowe Centrum Certyfikacji. Wszystkie klucze dla pieczęci elektronicznej są przetrzymywane zgodnie z wymaganiami określonymi w Podrozdziale 5.6 Zabezpieczenia Kryptograficzne.

3. Poczta Polska zapewnia sprawdzanie poprawności wygenerowanych pieczęci, jeżeli będzie korzystała z usługi zewnętrznego dostawcy usługi kwalifikowanej pieczęci.
4. Poczta Polska zapewnia, iż w takim przypadku, nie rzadziej niż raz na miesiąc, będzie sprawdzać, czy dostawca kwalifikowanej pieczęci elektronicznej znajduje się na liście Kwalifikowanych dostawców usługi zaufania.

#### **5.5. Usługa znakowania czasem**

1. Wszystkie dowody wystawiane przez Usługę RDE PP są znakowane czasem, w oparciu o zewnętrznego kwalifikowanego dostawcę kwalifikowanego znacznika czasu.
2. Poczta Polska zapewnia, iż codziennie dokonuje się kontroli aktualności wpisu dostawcy kwalifikowanego znacznika czasu na liście Kwalifikowanych dostawców usług zaufania.
3. Podpisana jest także umowa z zapasowym kwalifikowanym dostawcą usługi znakowania czasem na wypadek niedostępności podstawowej usługi.
4. Lista kwalifikowanych dostawców, z którymi współpracuje Poczta Polska w zakresie świadczenia Usługi RDE PP, udostępniona jest na stronie internetowej <https://edoreczenia.poczta-polska.pl/informacje/dostawcy-zewnetrzni/>.

#### **5.6. Zabezpieczenia kryptograficzne**

1. Prowadzony jest rejestr wszystkich kluczy kryptograficznych wraz z informacjami o zakresie ich stosowania oraz osobach odpowiedzialnych za wykorzystywanie i nadzór nad kluczami.
2. Wszelkie klucze kryptograficzne, w tym klucze certyfikatów dla zaawansowanej pieczęci elektronicznej, są przechowywane na inteligentnych urządzeniach kryptograficznych. Usługa pieczętowania jest obsługiwana przez stronę trzecią i połączona za pomocą bezpiecznych łączy. Tylko wartości hash komunikatów są przekazywane do usługi pieczęci.
3. Klucze prywatne Usługi RDE PP są generowane i przetwarzane w urządzeniach HSM posiadających jeden z certyfikatów:
  - 1) ISO/IEC 15408 (Common Criteria) dla poziomu EAL4 albo bezpieczniejszego,
  - 2) ISO/IEC 15408 (Common Criteria) dla poziomu określonego CEN EN 419 221-5:2018 – Protection Profiles for TSP Cryptographic Modules for Trust Services,
  - 3) FIPS PUB 140-2 dla poziomu 3 albo bezpieczniejszego,
  - 4) ISO/IEC 19790.

#### **6. Audyt zgodności i inne oceny**

Audyty są przeprowadzane w Systemie RDE w celu sprawdzenia zgodności postępowania Poczty Polskiej z wymaganiami nałożonymi na Kwalifikowanych dostawców usług zaufania określonych w Rozporządzeniu eIDAS oraz procedurami i procesami opisanymi w wewnętrznej dokumentacji Systemu RDE.

### **6.1. Częstotliwość i okoliczności oceny**

1. Audyt przeprowadzany jest:
  - 1) samodzielnie przez Audytorów Usługi RDE PP;
  - 2) zgodnie z wewnętrzną procedurą audytu dotyczącą usługi rejestrowanego doręczenia elektronicznego, lub
  - 3) raz na 2 lata przez zewnętrzną jednostkę oceniającą zgodność na podstawie art. 20 ust. 1 Rozporządzenia eIDAS („**Audyt zewnętrzny**”).
2. Audyt zewnętrzny może być przeprowadzony w każdym momencie na wniosek organu nadzoru w trybie art. 31 Ustawy w związku z art. 17 ust. 4 lit. e i art. 20 ust. 2 Rozporządzenia eIDAS.

### **6.2. Tożsamość i kwalifikacje audytora**

Audyt zewnętrzny przeprowadzany jest przez upoważnioną do tego rodzaju działalności instytucję krajową lub europejską, posiadającą akredytację do przeprowadzania audytów zgodności dostawców usług zaufania i spełniającą wymogi określone w normie ETSI EN 319 403.

### **6.3. Związek audytora z audytowaną jednostką**

Audytorzy nie mogą prowadzić działalności gospodarczej w zakresie świadczenia Usług zaufania, świadczyć Usług zaufania, być współnikami albo akcjonariuszami Dostawcy usług zaufania ani wykonywać obowiązków osoby reprezentującej lub członka rady nadzorczej albo komisji rewizyjnej tego dostawcy, a także pozostawać z tym dostawcą w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze.

### **6.4. Zagadnienia objęte audytem**

Do zagadnień objętych audytem należą w szczególności:

- 1) sprawdzenie wymagań organizacyjno-prawnych wynikających z Rozporządzenia eIDAS i wydanych decyzji wykonawczych do tego rozporządzenia;
- 2) monitorowanie i zapewnianie zgodności działalności z procedurami i politykami;
- 3) zabezpieczenia fizyczne;
- 4) zarządzanie bezpieczeństwem informacji;
- 5) stosowanie określonych zasad bezpieczeństwa przez Personel pełniący Role zaufane;
- 6) procedury świadczenia Usługi RDE PP;
- 7) zabezpieczenia oprogramowania i dostępu do sieci;
- 8) rejestry zdarzeń i procedury monitorowania systemu;
- 9) procedury sporządzania kopii zapasowych oraz ich odtwarzania;
- 10) realizacja procedur archiwizacji;
- 11) dokumentowanie zmian parametrów konfiguracyjnych Systemu RDE;
- 12) przegląd uprawnień w Systemie RDE.

### **6.5. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu**

1. Raporty audytów wewnętrznych i zewnętrznych przekazywane są Zarządowi Poczty Polskiej oraz Dyrektorowi BAC.
2. Zarząd Poczty Polskiej powołuje zespół osób w celu przygotowania w terminie określonym w raporcie pisemnego stanowiska Poczty Polskiej wobec wszelkich uchybień wskazanych w raportach, przy jednoczesnym określeniu sposobów i terminu usunięcia usterek. Informacja o usunięciu usterek przekazywana jest audytorowi.
3. W przypadku audytu zleconego przez ministra właściwego ds. informatyzacji, minister po zapoznaniu się z protokołem i zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez Poczta Polską powiadamia ten podmiot, o wynikach kontroli i w razie stwierdzenia nieprawidłowości wyznacza termin ich usunięcia, nie krótszy niż 14 dni.

### **6.6. Informowanie o wynikach audytu**

Informacje o wynikach audytu, w postaci raportu z jego przeprowadzenia lub podsumowania z takiego raportu, są udostępniane wyłącznie wewnątrznie upoważnionym osobom, jak: Zarząd Poczty Polskiej, Dyrektor BAC, Inspektor bezpieczeństwa.

## **7. Inne postanowienia**

### **7.1. Opłaty**

Z tytułu świadczenia Usługi RDE PP Poczta Polska pobiera opłaty według cennika publikowanego na stronie internetowej <https://bip.poczta-polska.pl/repozytorium/>.

### **7.2. Niedyskryminujące zastosowanie**

Dzięki wdrożeniu najlepszych rozwiązań w projektowaniu stron internetowych Poczta Polska oferuje Stronom Usługi RDE PP niedyskryminujący dostęp do Usługi RDE PP. Strony internetowe zostały przygotowane zgodnie ze standardem WCAG 2.0 (Web Content Accessibility Guidelines).

### **7.3. Odpowiedzialność finansowa**

1. Poczta Polska potwierdza, że zapewniono wystarczające środki finansowe na obsługę Usługi RDE PP i wypełnienie wszystkich zobowiązań dotyczących Usługi RDE PP.
2. Wszystkie uzgodnienia, niezbędne do świadczenia Usługi zaufania, z podwykonawcami, partnerami outsourcingowymi i stronami trzecimi, podlegają umowom i regulacjom obowiązującym w tym zakresie w Poczcie Polskiej.
3. Poczta Polska posiada ubezpieczenie odpowiedzialności cywilnej zgodne z wymaganiami Rozporządzenia Ministra Rozwoju i Finansów z dnia 19 grudnia 2016 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego dostawcy usług zaufania.

### **7.4. Poufność informacji**

1. Poczta Polska i osoby w niej zatrudnione bądź podmioty dokonujące czynności operacyjno-technicznych, w ramach obsługi Systemu RDE, są obowiązane do zachowania tajemnicy

przedsiębiorstwa wszelkich informacji powziętych w trakcie zatrudnienia lub wykonywania czynności jak powyżej także po ustaniu okresu zatrudnienia bądź umocowania do ich wykonywania. Szczegółowy zakres tajemnicy przedsiębiorstwa określony jest w oddzielnych wewnętrznych aktach prawnych Poczty Polskiej. W szczególności dotyczy to:

- 1) informacji wpływającej od/do Klientów Usługi RDE PP;
- 2) zapisów transakcji systemowych (zarówno w całości, jak też w postaci danych do przeglądu kontrolnego transakcji, tzw. rejestrów transakcji systemowych);
- 3) raportów audytu wewnętrznego oraz zewnętrznego;
- 4) informacji o podjętych środkach zabezpieczających sprzęt oraz oprogramowanie;
- 5) informacji o administrowaniu Usługami zaufania oraz projektowanymi zmianami w tym zakresie.

#### **7.5. Ochrona danych osobowych**

Poczta Polska przetwarza dane osobowe (w szczególności dane Klientów) zgodnie z obowiązującymi w tym zakresie przepisami prawa oraz wewnętrzną dokumentacją ochrony danych osobowych. Informacje na temat przetwarzania danych osobowych są dostępne w Regulaminie.

#### **7.6. Prawo do własności intelektualnej**

Prawa autorskie do Polityki posiada Poczta Polska. Polityka może być wykorzystywana wyłącznie w celu korzystania z oferowanych Usług zaufania. Wszelkie inne zastosowania, w tym wykorzystanie całości lub fragmentu dokumentu, wymaga uprzedniej pisemnej zgody Poczty Polskiej (pod rygorem nieważności), z tym, że Poczta Polska wyraża zgodę na powielanie i publikowanie w całości Polityki ze wskazaniem jej źródła.

#### **7.7. Zgodność z obowiązującym prawem**

Funkcjonowanie Poczty Polskiej w zakresie świadczenia Usługi RDE PP oparte jest na zasadach zawartych w Polityce oraz obowiązujących na terytorium Polski przepisach prawa.

#### **7.8. Zobowiązania i gwarancje**

##### **7.8.1. Zobowiązania Poczty Polskiej**

1. Poczta Polska gwarantuje, że:

- 1) postępuje zgodnie z prawem, a w szczególności nie narusza postanowień Rozporządzenia eIDAS, Ustawy wraz z przepisami wykonawczymi oraz nie narusza praw autorskich i licencyjnych stron trzecich;
- 2) świadczone Usługi zaufania są zgodne z powszechnie akceptowanymi normami i standardami, m.in.:
  - a) ETSI EN 319 401,
  - b) ETSI EN 319 521;

- 3) zatrudnia osoby pełniące Role zaufane, które posiadają wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych z Usługami zaufania, w tym w szczególności obejmujące dziedziny:
  - a) automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
  - b) mechanizmów zabezpieczania sieci i systemów teleinformatycznych,
  - c) kryptografii, pieczęci elektronicznych,
  - d) sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.
2. Wszystkie zegary funkcjonujące w ramach Usługi RDE PP są synchronizowane z międzynarodowym wzorcem czasu UTC, z dokładnością do 1 sekundy.

#### **7.8.2. Zobowiązania zewnętrznych podmiotów**

1. Celem realizacji Usług zaufania Poczta Polska współpracuje z PPUC, która jest dostawcą technicznego rozwiązania wykorzystywanego do świadczenia Usługi RDE PP oraz operatorem Systemu RDE. PPUC na podstawie umowy zawartej z Poczta Polską zobowiązana jest do przestrzegania wymagań wynikających z Polityki.
2. Wszyscy Kwalifikowani dostawcy usług zaufania współpracujący z Poczta Polską są zobowiązani spełniać wymagania bezpieczeństwa wynikające z Polityki.
3. Świadcząc Usługę RDE w oparciu o innych Dostawców usług zaufania, Poczta Polska zobowiązuje tych dostawców do spełnienia wymagań bezpieczeństwa wynikających z Polityki.

#### **7.8.3. Zobowiązania Klientów**

Klienci są zobowiązani do ochrony swoich danych dostępowych. Ponadto, Klienci ponoszą wyłączną odpowiedzialność za tworzenie lokalnych kopii zapasowych wysłanych i odebranych wiadomości.

#### **7.9. Ograniczenia odpowiedzialności**

1. Gwarancje Poczty Polskiej oparte są na ogólnych zasadach zawartych w Polityce oraz są zgodne z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi.
2. Poczta Polska nie ponosi odpowiedzialności finansowej zdefiniowanej w Polityce wobec innych osób trzecich, niebędących odbiorcami Usług zaufania dostarczanych przez Poczta Polską.
3. W celu nadzoru nad sprawnym działaniem Systemu RDE, rozliczania Klientów oraz Personelu pełniącego Role zaufane z ich działań, rejestrowane są wszystkie te zdarzenia występujące w systemie, które mają istotny wpływ na bezpieczeństwo funkcjonowania Systemu RDE.
4. W przypadku wymiany danych pomiędzy Dostawcą Usługi RDE PP, a Dostawcą usługi RDE:
  - 1) odpowiedzialność Poczty Polskiej w przypadku Kwalifikowanej Usługi RDE, której nadawca korzysta z usług Dostawcy Usługi RDE, rozpoczyna się od momentu przyjęcia Przesyłki do Systemu RDE, czyli od momentu potwierdzenia przyjęcia Przesyłki przez System RDE poprzez komunikat „SignalMessage typu Receipt”;

- 2) odpowiedzialność Poczty Polskiej w przypadku Kwalifikowanej Usługi RDE, której adresat korzysta z usług Dostawcy Usługi RDE, kończy się w momencie przekazania Przesyłki do Dostawcy Usługi RDE adresata, czyli w momencie potwierdzenia przyjęcia Przesyłki przez system Dostawcy Usługi RDE poprzez komunikat „SignalMessage typu Receipt”.
5. Przesyłki mogą być skanowane przez oprogramowanie antywirusowe. W przypadku wykrycia lub podejrzenia złośliwego oprogramowania podczas skanowania wystawiany jest dowód odrzucenia przesyłki A.2 albo B.2.
6. Poczta Polska nie ponosi odpowiedzialności w przypadku odrzucenia wiadomości przez Dostawcę Usług RDE, w tym za odrzucenie wiadomości w wyniku różnic w deklarowanych praktykach świadczenia usługi Poczty Polskiej i Dostawcy Usługi RDE.
7. Poczta Polska nie ponosi odpowiedzialności za treści przekazywane w ramach Usługi RDE PP, w tym w szczególności za treść korespondencji i załączników.

#### **7.10. Odszkodowania**

Odszkodowanie z tytułu odpowiedzialności cywilnej wobec Klienta wynika ze zobowiązań i gwarancji określonych w treści Polityki.

#### **7.11. Procedura wprowadzania zmian**

1. Niezależnie od prowadzonych w Poczcie Polskiej audytów, raz w roku odbywa się przegląd obowiązującej wersji Polityki. Wyznaczone przez Zarząd Poczty Polskiej osoby analizują treść Polityki w kierunku jej zgodności z wdrożonymi procedurami oraz wymaganiami zewnętrznymi.
2. Zmiany treści Polityki mogą być wynikiem zauważonych błędów, uaktualnień oraz sugestii zainteresowanych Stron Usługi RDE PP.
3. Jedynymi zmianami, które nie wymagają wcześniejszego informowania użytkowników, są zmiany wynikające z wprowadzenia korekt edycyjnych, zmiany w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie dokumentem, zmiany niemające rzeczywistego wpływu na znaczącą grupę użytkowników.
4. Po uprzednim poinformowaniu zainteresowanych Stron Usługi RDE PP, zmianom mogą podlegać dowolne elementy Polityki. Informacja o wszystkich istotnych, rozważanych zmianach w dokumencie jest przesyłana wszystkim zainteresowanym Stronom Usługi RDE PP w postaci informacji o miejscu dostępu nowej wersji Polityki.

#### **7.12. Zasady wykorzystywane w protokole AS4 przez Poczta Polską**

1. W celu wymiany danych z Systemem RDE w zakresie funkcjonowania z Kwalifikowaną Usługą RDE konieczne jest przeprowadzenie integracji systemu Dostawcy Usługi RDE z konektorem AS4.
2. Warunki integracji, o której mowa w ust. 1, udostępniane są Dostawcy Usługi RDE po uprzednim podpisaniu umowy o zachowaniu poufności pomiędzy Poczta Polską, a Dostawcą Usługi RDE.

3. Warunkiem koniecznym do uruchomienia komunikacji w protokole AS4 jest zakończenie z wynikiem pozytywnym testów integracyjnych przeprowadzonych przez Dostawcę Usługi RDE na środowisku testowym konektora AS4.