

Obowiązuje od 26 czerwca 2025 roku

Polityka świadczenia usługi i deklaracja praktyk dla usługi e-Archiwum w Poczcie Polskiej S.A.

Metryka dokumentu

Nazwa:	Polityka świadczenia usługi i deklaracja praktyk dla usługi e-Archiwum w Poczcie Polskiej S.A.		
Identyfikator dokumentu:	1/2025		
Wersja:	1.0	Autor:	Poczta Polska S.A.
Stron:	22	Data:	24.06.2025

Spis treści

1.	Wstęp	5
1.1.	Wprowadzenie	5
1.2.	Słownik	5
1.3.	Definicje Stron e-Archiwum	6
1.4.	Podstawowe elementy e-Archiwum	6
2.	Administracja i repozytorium	7
2.1.	Administracja polityką	7
2.2.	Repozytorium i publikacja dokumentu	7
3.	Identyfikacja i uwierzytelnienie	8
4.	Zabezpieczenia organizacyjne, operacyjne i fizyczne	8
4.1.	Zabezpieczenia fizyczne	9
4.1.1.	Lokalizacja i budynki	9
4.1.2.	Dostęp fizyczny	9
4.1.3.	Bezpieczeństwo środowiskowe	9
4.1.4.	Nośniki informacji	9
4.1.5.	Niszczenie informacji	9
4.1.6.	Kopie bezpieczeństwa	10
4.2.	Zabezpieczenia organizacyjne	10
4.2.1.	Role zaufane	10
4.2.2.	Role zaufane podlegające separacji obowiązków	11
4.2.3.	Zarządzanie incydentami	11
4.2.4.	Zarządzanie ryzykiem	12
4.2.5.	Nadzór nad Personelem pełniącym Role zaufane	12
4.2.5.1.	Kwalifikacje, doświadczenie, upoważnienia	12
4.2.5.2.	Weryfikacja Personelu	12
4.2.5.3.	Szkolenia	12
4.2.5.4.	Sankcje z tytułu nieuprawnionych działań	13
4.2.5.5.	Pracownicy kontraktowi	13
4.2.5.6.	Dokumentacja dla Personelu pełniącego Role zaufane	13
4.3.	Bezpieczna eksploatacja	14
4.3.1.	Rejestrowanie zdarzeń	14

4.3.2.	Tworzenie kopii zapasowych i odtwarzanie	14
4.3.3.	Archiwizacja zdarzeń	14
5.	Zabezpieczenia techniczne.....	15
5.1.	Zabezpieczenie sprzętu komputerowego	15
5.2.	Cykl życia zabezpieczeń technicznych	16
5.3.	Zabezpieczenia sieci	16
5.4.	Usługa pieczęci elektronicznej	17
5.5.	Usługa znakowania czasem	18
5.6.	Zabezpieczenia kryptograficzne	18
6.	Audyt zgodności i inne oceny.....	18
6.1.	Częstotliwość i okoliczność oceny	18
6.2.	Zagadnienia objęte audytem	19
6.3.	Działania podejmowane celem usunięcia usterek wykrytych podczas audytu	19
6.4.	Informowanie o wynikach audytu	19
7.	Inne postanowienia.....	19
7.1.	Opłaty.....	19
7.2.	Niedyskryminujące zastosowanie	20
7.3.	Odpowiedzialność finansowa	20
7.4.	Poufność informacji	20
7.5.	Ochrona danych osobowych.....	20
7.6.	Prawo do własności intelektualnej	20
7.7.	Zgodność z obowiązującym prawem	21
7.8.	Zobowiązania i gwarancje	21
7.8.1.	Zobowiązania Poczty Polskiej	21
7.8.2.	Zobowiązania Klientów	21
7.9.	Ograniczenia odpowiedzialności.....	21
7.10.	Odszkodowania	21
7.11.	Procedura wprowadzania zmian	21

1. Wstęp

1.1. Wprowadzenie

Niniejsza Polityka świadczenia usługi i deklaracja praktyk dla e-Archiwum w Poczcie Polskiej S.A. (dalej: „Polityka”) określa ogólne zasady stosowane przez Poczta Polską (dalej: „Poczta Polska”) w trakcie świadczenia e-Archiwum. Polityka definiuje Strony e-Archiwum, określa ich obowiązki i odpowiedzialność oraz obszary zastosowań jej regulacji. Ponadto określa rozwiązania, w tym techniczne i organizacyjne, wskazujące warunki zabezpieczeń dla e-Archiwum.

1.2. Słownik

1. **e-Archiwum** – usługa zaufania umożliwiająca przechowywanie plików w przestrzeni udostępnionej przez Poczta Polską, zapewniająca dowody archiwizacji plików, świadczona jako usługa dodatkowa powiązana ze świadczeniem PURDE, o której mowa w art. 3 pkt. 16 lit. m) Rozporządzenia eIDAS,
2. **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,
3. **Personel** – osoby zatrudnione w Poczcie Polskiej na podstawie umowy o pracę oraz osoby fizyczne świadczące osobiście usługi na rzecz Poczty Polskiej w oparciu o umowę cywilnoprawną (umowę o dzieło, umowę zlecenia, umowę o świadczenie usług), w tym członkowie Zarządu i Rady Nadzorczej Poczty Polskiej,
4. **Regulamin** – Regulamin świadczenia usługi e-Archiwum w Poczcie Polskiej S.A., dostępny na stronie internetowej <https://bip.poczta-polska.pl/repozytorium/> oraz w każdej placówce Poczty Polskiej,
5. **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
6. **System identyfikacji elektronicznej** – system identyfikacji elektronicznej, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym lub prawnym, a także osobom fizycznym reprezentującym osoby prawne;
7. **System e-Archiwum** – wszystkie elementy organizacyjne i techniczne zapewniające funkcjonowanie e-Archiwum,
8. **Środek identyfikacji elektronicznej** – materialna lub niematerialna jednostka zawierająca dane identyfikujące osobę i używana do celów uwierzytelniania dla usługi online,
9. **Ustawa** – ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej,
10. **Dyrektor BAC** – Dyrektor Biura Analiz i Cyfryzacji Procesów

1.3. Definicje Stron e-Archiwum

Nazwa strony	Opis
Dostawca e-Archiwum	Poczta Polska będąca samodzielnym dostawcą e-Archiwum
Dostawca usługi identyfikacji elektronicznej	Dostawca środka identyfikacji elektronicznej w ramach notyfikowanego krajowego schematu identyfikacji elektronicznej zapewniający użytkownikom usługi możliwość identyfikacji i uwierzytelnienia
Techniczny dostawca rozwiązania e-Archiwum	PPUC sp. z o.o. z siedzibą w Warszawie, funkcjonująca pod marką Envelo
Klient	Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, będąca posiadaczem ADE wraz z aktywnym e-Archiwum
Strona ufająca	Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, polegająca na zaufaniu do usługi zaufania jaką jest e-Archiwum, opisanego w Polityce
Użytkownik	Osoba fizyczna, mająca dostęp do e-Archiwum

1.4. Podstawowe elementy e-Archiwum

- e-Archiwum składa się z następujących elementów: dodawanie Pliku, usuwanie Pliku, przenoszenie Pliku, pobieranie Pliku i wystawianie dowodów:
 - dodawanie Pliku obejmuje następujące kroki:
 - identyfikację i uwierzytelnienie Użytkownika realizującego dodanie Pliku do e-Archiwum,
 - dodanie przez Użytkownika Pliku do e-Archiwum,
 - wystawienie dowodu dodania Pliku do e-Archiwum,
 - usuwanie Pliku obejmuje następujące kroki:
 - identyfikację i uwierzytelnienie Użytkownika realizującego usunięcie Pliku z e-Archiwum,
 - wybranie Pliku przeznaczonego do usunięcia,
 - potwierdzenie chęci dokonania usunięcia Pliku,
 - usunięcie Pliku,
 - przenoszenie Pliku obejmuje następujące kroki:
 - identyfikację i uwierzytelnienie Użytkownika realizującego przenoszenie Pliku pomiędzy folderami w usłudze e-Archiwum,

- b) wybranie Pliku do przeniesienia,
 - c) wybranie docelowego miejsca przeniesienia Pliku,
 - d) potwierdzenie chęci dokonania przeniesienia Pliku,
 - e) przeniesienie pliku,
- 4) pobieranie Pliku obejmuje następujące kroki:
- a) identyfikację i uwierzytelnienie Użytkownika realizującego pobranie Pliku z e-Archiwum,
 - b) wybranie Pliku przeznaczonego do pobrania,
 - c) pobranie Pliku,
- 5) wystawianie dowodów z tytułu:
- a) dodanie Pliku,
 - b) zmiany nazwy Pliku.
2. Wystawione dowody w zakresie dodania Pliku i zmiany nazwy są zabezpieczone pieczęcią elektroniczną oraz znakowane czasem. Poczta Polska udostępnia Klientom dowody wytworzone w procesie świadczenia e-Archiwum przez okres nie krótszy niż 24 miesiące.
3. Informacje o pliku w wystawianych przez Dostawcę e-Archiwum dowodach są tworzone z wykorzystaniem funkcji skrótu SHA3-512.
4. Niezależnie od utraty danych z powodów technicznych lub innych, Poczta Polska zapewnia utrzymanie dokumentów i danych, wynikających z art. 17 ust. 1 Ustawy, przez okres 20 lat od momentu ich wytworzenia.

2. Administracja i repozytorium

2.1. Administracja polityką

1. Poczta Polska wskazuje Dyrektor 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 e-Archiwum, 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,
 - 4) innych dokumentach przeznaczonych do publikacji na podstawie Polityki, jeśli takie wskazano.
2. Dokumenty umieszczone w repozytorium są publicznie dostępne pod adresem www.bip.poczta-polska.pl/repozytorium.

3. Wszelkie zmiany Polityki są archiwizowane, a ich zmienione wersje publikowane na bieżąco (každorazowo, 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 e-Archiwum korzysta z zewnętrznego procesu identyfikacji elektronicznej. W ramach e-Archiwum nie jest wydawany środek uwierzytelniający.
2. Każdy adres do doręczeń elektronicznych zapewnia jednoznaczną identyfikację Użytkownika.
3. W ramach e-Archiwum dopuszcza się następujące sposoby identyfikacji i uwierzytelniania:
 - 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 e-Archiwum 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 uwierzytelnienia w systemie teleinformatycznym banku krajowego lub innego przedsiębiorcy, spełniającym warunki ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
4. Identyfikacja elektroniczna przeprowadzana jest za każdym razem przed wejściem do e-Archiwum.
5. 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 e-Archiwum.
2. Wewnętrzny dokument dotyczący polityki bezpieczeństwa informacji jest komunikowany każdej osobie pełniącej Rolę zaufaną w zakresie e-Archiwum świadczonej przez Poczta Polską, 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 e-Archiwum 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 e-Archiwum 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 e-Archiwum posiadają tylko osoby upoważnione.
5. Weryfikacja uprawnień dostępu do pomieszczeń realizowana jest w oparciu o elektroniczny system kontroli dostępu umożliwiający identyfikację i rozliczalność osób upoważnionych.

4.1.3. Bezpieczeństwo środowiskowe

1. W przypadku zaniku zasilania podstawowego, e-Archiwum przechodzi na zasilanie awaryjne poprzez UPS, czyli urządzenie, którego funkcją jest nieprzerwane zasilanie urządzeń elektronicznych e-Archiwum.
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 zainstalowano 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 ognioodpornych. 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 centrum podstawowym.
2. Tworzenie kopii zapasowych weryfikowane jest przez Operatora systemu.

4.2. Zabezpieczenia organizacyjne

4.2.1. Role zaufane

1. Osoby sprawujące nadzór nad e-Archiwum pełnią określone Role zaufane, które zaprezentowano w poniższej tabeli.

Nazwa Roli zaufanej	Zakres głównych obowiązków
Dyrektor BAC	▪ Zapewnienie prawidłowej organizacji i funkcjonowania e-Archiwum. Wdrożenie/Wdrażanie postanowień Polityki. ▪ Zapewnienie zgodności e-Archiwum z prawem oraz standardami normalizacyjnymi. ▪ Nadzorowanie zapewnienia ciągłości działania oraz zapewnienie realizacji planu zakończenia działalności.
Kierownik komórki organizacyjnej odpowiedzialny za systemy usług zaufania	▪ Zarządzanie działem i nadzorowanie jego funkcjonowania. ▪ Zapewnienie prawidłowej organizacji i funkcjonowania e-Archiwum. ▪ Realizacja kierunków rozwoju usług. ▪ Utrzymanie aktualności planu zakończenia działalności.
Operator systemu	▪ Instalowanie, konfigurowanie i zarządzanie systemami oraz sieciami teleinformatycznymi wykorzystywanymi na potrzeby świadczenia e-Archiwum. ▪ Dbalność o operacyjne aspekty świadczenia e-Archiwum. ▪ Wykonywanie procedur i instrukcji operacyjnych. ▪ Realizacja procedur utrzymania e-Archiwum.
Administrator systemu	▪ Zapewnienie współpracy z dostawcą (dostawcami), w szczególności z PPUC sp. zo.o. i umiejscowionymi u tego dostawcy Operatorami systemu. ▪ Operacyjne czynności w zakresie zarządzania kluczami.
Inspektor bezpieczeństwa	▪ Zapewnienie bezpieczeństwa procesu w ramach świadczonego e-Archiwum. ▪ Wdrażanie i realizacja postanowień wewnętrznego dokumentu dotyczącego polityki bezpieczeństwa informacji, w tym m.in.: ✓ zapewnienie zarządzania ryzykiem, ✓ nadzorowanie procesu zarządzania incydentami, ✓ nadzorowanie bezpieczeństwa fizycznego, bezpieczeństwa sieci oraz zarządzania ciągłością działania,

	✓ zarządzanie uprawnieniami w zakresie e-Archiwum.
Audytor	▪ Przeglądanie archiwów i dzienników zdarzeń e-Archiwum. ▪ Analizowanie zdarzeń i incydentów dotyczących e-Archiwum. ▪ Rekomendowanie działań naprawczych i profilaktycznych. ▪ Kontrola wdrożonych mechanizmów i środków bezpieczeństwa.
Koordynator ds. wdrożenia eUsług	▪ Koordynowanie działań dotyczących e-Archiwum.
Inspektor ds. weryfikowania tożsamości	▪ Odpowiedzialność za proces weryfikacji tożsamości nadawcy i odbiorcy i zgodność jego rzeczywistego przebiegu z przyjętymi założeniami.

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 poszczególnych Roli zaufanej w e-Archiwum.

4.2.2. Role zaufane podlegające separacji obowiązków

1. Role zaufane wyodrębnione w ramach Personelu zapobiegają nadużyciom, przy korzystaniu z e-Archiwum.
2. Każdej osobie odpowiedzialnej za eksploatację Systemu e-Archiwum wykorzystywanego do świadczenia e-Archiwum 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 e-Archiwum.
2. Poczta Polska bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu incydu, 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 e-Archiwum 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 e-Archiwum.

4.2.5. Nadzór nad Personelem pełniącym Role zaufane

4.2.5.1. Kwalifikacje, doświadczenie, upoważnienia

Osoby uczestniczące w świadczeniu e-Archiwum, 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 e-Archiwum lub poufności danych Użytkownika, 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 e-Archiwum,
- 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 e-Archiwum 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 e-Archiwum,
 - 6) oprogramowania systemu komputerowego e-Archiwum,
 - 7) procedur realizowanych po awariach lub katastrofach Systemu e-Archiwum,
 - 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 e-Archiwum przez Poczta Polską.

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 e-Archiwum 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 zewnętrznymi 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 e-Archiwum.
2. Zakres odpowiedzialności osób fizycznych świadczących osobiście usługi na rzecz Poczty Polskiej lub PPUC sp. z o.o. 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 umożliwia członkom swojego Personelu pełniącym Role zaufane dostęp do następujących dokumentów:

- 1) Polityki,
- 2) procedur eksploatacyjnych (tylko dla Ról zaufanych) w zakresie obsługi Systemu e-Archiwum,
- 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 e-Archiwum 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 e-Archiwum 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 Użytkowników e-Archiwum,
 - d) czynności związane z obsługą Użytkowników, w tym dowody w zakresie m.in. dodania Pliku,
 - 2) logi systemowe z serwerów i stacji roboczych wchodzących w skład Systemu e-Archiwum,
 - 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 e-Archiwum, awariami Systemu e-Archiwum i awariami sprzętu, działaniami zapory i routera oraz próbami dostępu do Systemu e-Archiwum.
2. Ponadto 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. Zapisy zdarzeń są kopiowane zgodnie z harmonogramem tworzenia kopii bezpieczeństwa Systemu e-Archiwum. 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.

4.3.3. Archiwizacja zdarzeń

1. W ramach e-Archiwum archiwizacji podlegają w szczególności:
 - 1) dane identyfikacyjne Użytkowników lub Personelu pełniącego Role zaufane,

- 2) dane uwierzytelniające Użytkowników lub Personelu pełniącego Role zaufane,
 - 3) dowód, że tożsamość Użytkownika e-Archiwum została pierwotnie zweryfikowana,
 - 4) logi operacji e-Archiwum, weryfikacji tożsamości dodającego, zmieniającego lub pobierającego Pliki,
 - 5) dowody na to, że Plik nie został zmodyfikowany podczas transmisji i archiwizacji,
 - 6) tokeny znaczników czasu odpowiadające dacie i godzinie dodania, pobrania oraz modyfikowania Pliku, stosownie do przypadku,
 - 7) Polityka oraz jej historyczne wersje,
 - 8) inne dokumenty umieszczone w repozytorium zgodnie z zapisami Polityki.
2. Archiwum zawiera również wszelkie dokumenty papierowe, związane ze świadczeniem e-Archiwum, których okres przechowywania wynosi 20 lat zgodnie z art. 17 ust. 1 Ustawy, z zastrzeżeniem art. 20 ust. 1 Ustawy.
 3. Poczta Polska zapewnia poufność, integralność i dostępność tworzonych rejestrów zdarzeń.
 4. Zapisy dotyczące funkcjonowania e-Archiwum są udostępniane, jeśli jest to wymagane, w celu udokumentowania prawidłowego działania e-Archiwum dla celów postępowania sądowego.

5. Zabezpieczenia techniczne

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

5.1. Zabezpieczenie sprzętu komputerowego

1. Wymagania techniczne określone w niniejszym rozdziale odnoszą się do kontroli zabezpieczeń pojedynczego komputera oraz zainstalowanego na nim oprogramowania w ramach Systemu e-Archiwum.
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 e-Archiwum wyposażone są w następujące funkcje zabezpieczające:
 - 1) obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji
 - 2) uznaniową kontrolę dostępu,
 - 3) możliwość prowadzenia audytu zabezpieczeń,
 - 4) wymuszanie separacji obowiązków wynikających z pełnionych ról,
 - 5) wymuszanie wylogowania Personelu po okresie bezczynności,
 - 6) identyfikację i uwierzytelnienie Personelu
 - 7) kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenie baz danych,

- 8) archiwizowanie danych dla potrzeb audytu,
- 9) bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie Personelu,
- 10) mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,
- 11) 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 e-Archiwum sprawuje Inspektor bezpieczeństwa. Zatwierdza on konfigurację Systemu e-Archiwum 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 e-Archiwum, integralność jego zasobów oraz zachowanie poufności danych.
3. Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania Systemu e-Archiwum, 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 e-Archiwum 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 e-Archiwum i wymaga jej weryfikacji przez osobę inną od tej, która wprowadzała daną zmianę.
6. Aktualna konfiguracja Systemu e-Archiwum, jak również modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Zastosowane w Systemie e-Archiwum 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 e-Archiwum sprawują Administratorzy systemu.
2. Sieć w ramach e-Archiwum 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 e-Archiwum, zlokalizowanymi w różnych ośrodkach, jest realizowana za pomocą szyfrowanych kanałów, zapewniających identyfikację Użytkowników e-Archiwum 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 e-Archiwum 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 6 miesięcy) 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 e-Archiwum, 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.
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 e-Archiwum (po konfiguracji i po aktualizacji lub modyfikacjach infrastruktury lub aplikacji), Poczta Polska zapewnia przeprowadzenie testów penetracyjnych oraz gromadzi dowody z prowadzonych testów.

5.4. Usługa pieczęci elektronicznej

1. Wszystkie Pliki są zabezpieczone za pomocą usługi zaawansowanej pieczęci elektronicznej. Integralność Pliku i związanych z nią metadanych jest chroniona podczas transmisji i przechowywania, w szczególności w przypadku wymiany między rozproszonymi komponentami Systemu e-Archiwum, a także w pamięci masowej. Ochrona integralności jest realizowana poprzez weryfikację pieczęci elektronicznych dla dokumentów wgrywanych i pobieranych, 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 rozdziale 5.6 Zabezpieczenia Kryptograficzne.

3. Poczta Polska zapewnia sprawdzanie poprawności wygenerowanych pieczęci, jeżeli będzie korzystać 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 e-Archiwum 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.

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 e-Archiwum są generowane i przetwarzane w urządzeniach HSM posiadających jeden z certyfikatów:
4. ISO/IEC 15408 (Common Criteria) dla poziomu EAL4 albo bezpieczniejszego,
5. ISO/IEC 15408 (Common Criteria) dla poziomu określonego CEN EN 419 221-5:2018 – Protection Profiles for TSP Cryptographic Modules for Trust Services,
6. FIPS PUB 140-2 dla poziomu 3 albo bezpieczniejszego,
7. ISO/IEC 19790.

6. Audyt zgodności i inne oceny

Audyty przeprowadzane są w Systemie e-Archiwum w celu sprawdzenia zgodności postępowania Poczty Polskiej z procedurami i procesami opisanymi w wewnętrznej dokumentacji Systemu e-Archiwum.

6.1. Częstotliwość i okoliczność oceny

Audyt przeprowadzany jest:

- 1) samodzielnie przez Audytorów e-Archiwum,

- 2) zgodnie z wewnętrzną procedurą audytu dotyczącą e-Archiwum.

6.2. Zagadnienia objęte audytem

Do zagadnień objętych audytem należą w szczególności:

- 1) monitorowanie i zapewnianie zgodności działalności z procedurami i politykami,
- 2) zabezpieczenia fizyczne,
- 3) zarządzanie bezpieczeństwem informacji,
- 4) stosowanie określonych zasad bezpieczeństwa przez Personel,
- 5) procedury świadczenia e-Archiwum,
- 6) zabezpieczenia oprogramowania i dostępu do sieci,
- 7) rejestry zdarzeń i procedury monitorowania systemu,
- 8) procedury sporządzania kopii zapasowych oraz ich odtwarzania,
- 9) realizacja procedur archiwizacji,
- 10) dokumentowanie zmian parametrów konfiguracyjnych Systemu e-Archiwum,
- 11) przegląd uprawnień w Systemie e-Archiwum.

6.3. Działania podejmowane celem usunięcia usterek wykrytych podczas audytu

1. Raporty audytów wewnętrznych i zewnętrznych przekazywane są Zarządowi Poczty Polskiej oraz Dyrektora 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

6.4. 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 e-Archiwum, Poczta Polska pobiera opłaty według cennika publikowanego na stronie internetowej www.bip.poczta-polska.pl/repozytorium.

7.2. Niedyskryminujące zastosowanie

Dzięki wdrożeniu najlepszych rozwiązań w projektowaniu stron internetowych Poczta Polska oferuje Klientom e-Archiwum niedyskryminujący dostęp do e-Archiwum. 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 e-Archiwum i wypełnienie wszystkich zobowiązań dotyczących e-Archiwum.
2. Wszystkie uzgodnienia, niezbędne do świadczenia e-Archiwum, z podwykonawcami, partnerami outsourcingowymi i stronami trzecimi, podlegają umowom i regulacjom obowiązującym w tym zakresie w Poczcie Polskiej.

7.4. Poufność informacji

Poczta Polska i osoby w niej zatrudnione bądź podmioty dokonujące czynności operacyjno-technicznych, w ramach obsługi Systemu e-Archiwum, są obowiązane do zachowania tajemnicy przedsiębiorstwa wszelkich informacji powziętych w trakcie zatrudnienia lub wykonywania czynności 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 e-Archiwum,
- 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 przedsięwziętych 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 użytkowników e-Archiwum) 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. 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 e-Archiwum 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 praw autorskich i licencyjnych stron trzecich,
 - 2) e-Archiwum jest świadczone zgodnie z powszechnie akceptowanymi normami i standardami.
2. Wszystkie zegary funkcjonujące w ramach e-Archiwum są synchronizowane z międzynarodowym wzorcem czasu UTC, z dokładnością do 1 sekundy.

7.8.2. Zobowiązania Klientów

Klienci są zobowiązani do ochrony swoich danych dostępowych. Ponadto, Klienci ponoszą wyłączną odpowiedzialność za tworzenie lokalnych kopii plików przesłanych do e-Archiwum.

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 podnosi odpowiedzialności finansowej zdefiniowanej w Polityce wobec innych osób trzecich, niebędących odbiorcami e-Archiwum dostarczanej przez Poczta Polską.
3. W celu nadzoru nad sprawnym działaniem Systemu e-Archiwum, rozliczania Klientów oraz Personelu z ich działań, rejestrowane są wszystkie te zdarzenia występujące w systemie, które mają istotny wpływ na bezpieczeństwo funkcjonowania Systemu e-Archiwum.

7.10. Odszkodowania

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

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 e-Archiwum.
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 e-Archiwum, zmianom mogą podlegać dowolne elementy Polityki. Informacja o wszystkich istotnych, rozważanych zmianach w dokumencie jest przesyłana wszystkim zainteresowanym Stronom e-Archiwum w postaci informacji o miejscu dostępu nowej wersji Polityki.