PIXA

Certificate Policy

Date: January 02, 2026

Version: 1.0.0

Contents

Document History

Document Change Control

Version	Release Date	Author	Status & Description
1.0.0	January 5, 2026	Patrick Mercier	Initial CP for PIXA

Acknowledgements

This PIXA PKI Policy Group CPS endorses in whole or in part the following industry standards:

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
- The ISO 1-7799 standard on security and infrastructure

From Section 9.5 of this CP:
This Certificate Policy (CP) incorporates material derived from the *Microsoft PKI Services Certificate Policy (CP)* Version 3.1.9, published April 21, 2025. The Microsoft document is licensed under the Creative Commons Attribution–NoDerivatives 4.0 International License (CC BY-ND 4.0). PIXA retains all intellectual property rights in and to this adapted CP, which is specific to PIXA and includes additional original material.

microsoft.com/pkiops/docs/repository.htm

1. Introduction

1.1. Overview

This document is the Certification Policy (CP) that defines the procedure and operational requirements governing the lifecycle management of PIXA PKI Policy Group Certification Authority (CA) solutions and services for affiliated entities, Applicants, Subscribers, and Relying Parties. PIXA PKI Policy Group requires entities to adhere to this CP when issuing and managing digital certificates within PIXA PKI Services PKI hierarchy. This MAY include services managed by PIXA PKI Policy Group as well as other groups within PIXA responsible for managing trusted and untrusted CAs. Each PKI service is required to have an associated Certification Practice Statement (CPS) that adheres to this CP.

Important documents that accompany this CP include a CPS and associated Subscriber and Relying Party Agreements in the form of an appropriate use agreement found at HTTPS://HRDOCS. PIXA MAY publish additional Certificate Policies or Certification Practice Statements, as necessary, to describe other products or service offerings.

1.2. Document Name and Identification

This document is formally named the “PIXA – Certificate Policy” (referred to as “CP”). PIXA Certification Authorities issue certificates in accordance with the policy and practice requirements of this document. The Object Identifier (OID) for this CP is: 1.3.6.1.4.1.64104.2.1

1.3. PKI Participants

1.3.1. Certification Authorities

The term Certification Authority (CA) collectively refers to an entity or organization that is responsible for the authorization, issuance, revocation, and management of a Certificate. The term equally applies to Root CAs and Subordinate CAs. The CA hierarchy structure and specific practices SHALL be specified within the relevant Certification Practice Statement (CPS).

1.3.2. Registration Authorities

A Registration Authority (RA) is any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the Certificate Application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

1.3.3. Subscribers

A Subscriber is an individual or end-entity (person, device, or applications) that has been issued a Certificate and is authorized to use the Private Key that corresponds to the Public Key in the Certificate.

1.3.4. Relying Parties

A Relying Party is an individual or entity that acts in reliance on a Certificate or digital signature associated with a Certificate.

1.3.5. Other Participants

Other groups that have participated in the development of this Certificate Policy and respective Certification Practice Statement (CPS).

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

Certificates issued under this Certificate Policy SHALL only be used for the purposes identified by the Issuing CA in its Certification Practice Statement and for the purposes designated in the key usage and/or extended key usage fields found in the certificate.

All end-entity certificates issued within this CA hierarchy are technically constrained for use. This is done either by the inclusion of at least one extended key usage extension in the end-entity certificate, or by inclusion of one or more extended key usage extensions in the issuing CA's certificate.

The following certificate class options and assurance levels are available to Applicants in the form of CA and end-entity Certificates issued by the PIXA CAs. The Issuing CA will assess the risk and apply the appropriate rating.

Low Assurance - Certificates of this class provide a low level of assurance to publicly available products and services.

Medium Assurance - This level is relevant where risks and consequences of compromise are significant. Medium assurance CAs include but are not limited to intermediate production CAs (i.e. non-root CAs). CAs operating under this policy are hosted and managed by PIXA PKI Policy Group and employ pre-defined and approved fulfillment practices to provision CA and end-entity production certificates to Applicants.

High Assurance - This level is relevant where risks and consequences of compromise are high. High assurance CAs include but are not limited to root and intermediate CAs. CAs operating under this policy are hosted and managed by PIXA PKI Policy Group and employ pre-defined and approved fulfillment practices to provision CA production certificates to Applicants.

1.4.2. Prohibited Certificate Uses

Use of certificates in violation of Section 1.4.1 is unauthorized and prohibited.

Certificates MUST only be used to the extent permitted with applicable laws. CA Certificates MUST NOT be used for any functions except CA functions.

In addition, end-user Subscriber Certificates SHALL NOT be used as CA Certificates.

1.5. Policy Administration

1.5.1. Organization Administering the Document

The Policy Managing Authority is responsible for the maintenance of this CP.

1.5.2. Contact Person

Contact Information is listed below:

PIXA Policy Group

info@pixa.ca

1.5.3. Person Determining CPS Suitability for the Policy

The PIXA PKI Policy Management Group determines the suitability of the CPS to this CP.

1.5.4. CPS Approval Procedures

The PIXA PKI Policy Management Group reviews and approves any changes to the CPS that is compliant with this CP. Updates to CP or CPS documents SHALL be made available by publishing new versions at https://pki.pixasecurity.ca.

1.6. Definitions and Acronyms

Upper Case terms and acronyms, not specified herein, are defined in the CA/B Forum's Baseline Requirements (BR) or the CA/B Forum's Code Signing Baseline Requirements.

1.6.1. Definitions

- Baseline Requirements (BR) – An integrated set of technologies, protocols, identity proofing, lifecycle management, and auditing requirements issued by the CA/Browser Forum and available at cabforum.org.
- CA/Browser Forum (CA/B Forum) – A consortium of certification authorities, vendors of Internet browser software, operating systems, and other PKI-enabled applications that
- Certificate – digital record that contains information such as the Subscriber's distinguished name and Public Key, and the signer's signature and data.
- Certificate Application – a request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
- Certificate Request – an application for a new Certificate or a renewal of a Certificate.
- Certificate Revocation List (CRL) – periodically published listing of all certificates that have been revoked for use by Relying Parties.
- Certificate Signing Request (CSR) – a message sent to the certification authority containing the information required to issue a digital certificate
- Certification Authority (CA) – an entity or organization that is responsible for the authorization, issuance, revocation, and management of a certificate. The term equally applies to Roots CAs and Subordinate CAs.
- Certificate Owner – Parties designated by business process owners to be associated with and/or have responsibility for specified issued certificates.
- Certificate Policy (CP) – A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

- Certification Practice Statement (CPS) – One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

1.6.2. Acronyms

Term	Definition
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
TLS	Transport Layer Security
TTL	Time To Live

1.6.3. References

CA/Browser Forum Network and Certificate Systems Security Requirements (“NCSSRs”) or Network Security Requirements (“NSRs”)

FIPS 140-3, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, March 22, 2019.

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.

X.509, Recommendation ITU-T X.509 (10/2023) | ISO/IEC 9594-8/Core2 (Common), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

1.6.4. Conventions

The key words “MUST”, “MUST NOT”, "REQUIRED", "SHALL", "SHALL NOT", “SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements SHALL be interpreted in accordance with RFC 2119.

2. Publication and Repository Responsibilities

2.1. Repositories

A public Repository of CA information and associated policy documents is located at https://pki.pixasecurity.ca

2.2. Publication of Certification Information

This CP conforms to the Internet Engineering Task Force (IETF) RFC 3647 standards for the creation of Certificate Policy (CP) and Certification Practices Statement (CPS) documents. This document SHALL not be used for the issuance and management of Publicly trusted TLS certificates and as such may not adhere to the BRs for public/web trust.

In the event of an inconsistency between this document and the governing industry requirements, this document takes precedence.

A web-based repository is available on a 24x7 basis to all Relying Parties who wish to access this CP or other information from PIXA PKI Policy Group. The repository SHALL contain the current version of this CP, CPS, a fingerprint of the established Root CAs, current CRLs, and other information relevant to Subscribers and Relying Parties.

The CA SHALL host internal test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates, specifically Client or Server Authentication certificates, that chain up to the PIXA PKI Policy Group's root CA. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are

(i) valid,
(ii) revoked, and
(iii) expired.

2.3. Time or Frequency of Publication

The CA SHALL annually review their CP and CPS and compare them with the CA/B Forum's TLS Baseline Requirements and the CA/B Forum's Code Signing Baseline Requirements for any modifications.

Updates SHALL be published annually, in accordance with Section 1.5, and the document version number SHALL be incremented to account for the annual review and potential content revisions.

New versions of this CP and respective CPS documents will become effective immediately for all participants listed in Section 1.3. The CA offers CRLs showing the revocation of PIXA PKI Policy Group Certificates and offers status checking through the online repository. CRLs will be published in accordance with Section 4.9.6 and Section 4.9.7.

2.4. Access Controls on Repositories

CAs SHALL NOT limit access to this CP, their CPS, Certificates, CRLs and Certificate status information. CAs SHALL however implement controls to prevent unauthorized adding, modifying or deleting of repository entries.

3. Identification and Authentication

3.1. Naming

3.1.1. Naming Convention

Certificates SHALL be issued in accordance with the X.509 standard. CA Certificates SHALL generate and sign certificates containing a compliant Distinguished Name (DN) in the Issuer and Subject name fields; the DN MAY contain domain component elements. The

Subject Alternative Name (SAN) MAY be used. Naming values for domain-validated and organization-validated TLS Certificates conform with the governing CA/Browser Forum Guidelines published at www.cabforum.org. The certificate profiles for specifying names SHALL conform with requirements in Section 7.

3.1.2. Acceptable Subscriber Names

While PIXA has no explicit requirements for this item, it is helpful for names to be meaningful, unique or require rules for interpretation, when such requirements arise, supporting documentation and registration in the service Catalog for PIXA.

3.1.3. Pseudonyms

No requirement

3.1.4. Recognition, Authentication and Role Trademarks

Certificate Applicants SHALL NOT use names in their Certificate Application or Certificate Request that infringe upon the intellectual property rights of entities outside of their authority.

3.2. Initial Identity Validation

3.2.1. Prove Access to Private Key

The registration and/or Issuance process SHALL involve procedures in which the Applicant demonstrates possession of the Private Key by using a self-signed PKCS#10 request, other equivalent cryptographic mechanism, or a different method approved by the Issuing CA.

3.2.2. Authentication of Organization Identity

The Issuing CA SHALL verify the identity of the organization and authority of the Applicant to request Certificates on behalf of the organization, in accordance with procedures set forth in PIXA procedures which will include the use of RAs or the submission of a Service Request.

Requests containing wildcards (*) will be summarily denied.

3.2.3. Validation of Authority

Requests submitted outside of the authorized RA MUST be completed through the submission of a Service Request which will initiate the required authentication processes. Approval of the Service Request will constitute validation of identity and authority.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-Key

Issuing CAs SHALL treat certificate re-key requests identical to applications for new certificates and perform the same identity-proofing processes as described in Section 3.2. Routine re-key of the issuing CA certificates SHALL be performed in accordance with the established Key Generation process in Section 6.1 of this CP.

3.3.2. Identification and Authentication for Re-Key After Revocation

Revoked or Expired Certificates SHALL require a new enrollment. Applicants MUST submit a new Certificate Request and be subject to the same Identification and Authentication requirements as first-time Applicants, as specified in Section 3 of this CP.

3.4. Identification and Authentication for Revocation Request

A Certificate Revocation Request that is submitted electronically MAY be authenticated and approved, providing the request comes from the Subscriber or an approved authority.

4. Certificate Life-cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Only employees of PIXA or devices managed by PIXA may apply for a Certificate. Contractors for PIXA may be granted special dispensation to submit applications as employees through the existence of user credentials within an approved RA.

Any applications by entities that are not employed by or managed by PIXA must have their application sponsored by an authorized PIXA employee. Approval for the submission will be granted or denied by the PIXA PKI Policy Group

4.1.2. Enrollment Process and Responsibilities

For enrollment not completed automatically via an approved RA, the CA SHALL obtain a Service Request from the applicant.

The applicant can submit an electronic CSR which will include the number of the approved Service Request as the OU field of the DN.

One Service Request is required for each certificate requested.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

4.2.1.1. Entities managed by PIXA

Users and Devices managed via PIXA Active Directory Domain Services or Entra ID as approved Registration Authorities will be identified and authorized based on authoritative information provided by the RA.

4.2.1.2. Un-managed Entities

The Certificate Request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with the Baseline Requirements, CP and CPS. In cases where the Certificate Request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's SubjectAltName extension.

Certificate Applications are reviewed and processed, per the Identification and Authentication requirements in Section 3.2. The CA MAY use the documents and data acquired in Section 3.2 to verify certificate information or reuse previous validations, provided that The CA obtained the data or document from a source specified under Section 3.2 or completed the validation itself in compliance with the timeframe specified in the appropriate CPS.

Certificate requests that are identified as “High Risk” SHALL be subject to additional verification activities, as outlined in documented procedures, prior to approving the request.

The CA MAY delegate the performance of all or any part of a requirement of this CP to an Affiliate, a RA, or subcontractor, provided that the process employed by the CA provides at least the same level of assurance as the CA’s own processes. Affiliates and/or RAs MUST comply with the qualification requirements of Sections 5.2.4, 5.3.2, and 5.3.3 in this CP.

4.2.2. Approval or Rejection of Certificate Applications

Submitted Certificate Applications MUST be reviewed and approved by the issuing CA or appointed RA prior to issuance.

The Certificate Application MAY be rejected for any of, but not limited to, the following reasons:

- Applicant or Subscriber information is unable to be verified;
- The CA deems the certificate issuance MAY negatively impact the CA’s business or reputation;
- Failure to consent to the Subscriber Agreement;
- Failure to provide an approved Service Request tracking number;
- Mismatches in submitted values as compared to the Service Request

The CA reserves the right not to disclose reasons for refusal.

4.2.3. Time to Process Certificate Applications

Certification applications SHALL be processed within PIXA Service Level Targets, in accordance with the CPS. The CA SHALL NOT be responsible for processing delays initiated by the Applicant or from events outside of the CA’s control.

4.2.4. Verification of DNS Records

PIXA has no requirements.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

The source of the Certificate Request SHALL be verified before issuance. Certificates are generated, issued and distributed only after the CA or RA performs the required identification and authentication steps in accordance with Section 3. Certificates SHALL be checked to ensure that all fields and extensions are properly populated. Exceptions to this CP MUST be approved by the PIXA PKI Policy Group

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

Upon issuance, Subscribers MAY be notified via an email or another agreed upon method with information about their issued Certificate as defined in the CPS.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

A Subscriber's/Applicant's, or Applicant Representative's receipt of a Certificate and subsequent use of the key pair and Certificate constitutes Certificate acceptance.

4.4.2. Publication of the Certificate by the CA

Certificates SHALL be published in a database.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

PIXA has no requirements for this item.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Use of the Private Key corresponding to the Public Key in the Certificate SHALL only be permitted once the Subscriber, or Applicant Representative, has agreed to the Subscriber agreement and accepted the Certificate.

See Section 9.6.3, provisions 2 (Protection of Private Key) and 4 (Use of Certificate).

Subscribers and CAs SHALL use their Private Keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the Certificates issued to them.

Subscribers SHALL protect their Private Keys from unauthorized use and discontinue use of the Private Key following expiration or revocation of the Certificate.

Subscribers SHALL contact the issuing entity if Private Key is compromised.

4.5.2. Relying Party Public Key and Certificate Usage

Relying parties SHALL use Public Key certificates and associated Public Keys for the sole purposes as constrained by the CP or respective CPS and Certificate extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates. Relying Parties are subject to the terms of the Relying Party Agreement on the public repository and responsibly verify the validity of the Certificate, including revocation status, prior to trusting any Certificate.

4.6. Certificate Renewal

4.6.1. Circumstance for Certificate Renewal

Subscribers are responsible for the renewal of Certificates to maintain service continuity.

4.6.2. Who May Request Renewal

Certificate renewals MAY be requested by the Subscriber or an authorized agent, as long as the renewal request meets the requirements set forth in this CP and the supporting CPS.

4.6.3. Processing Certificate Renewal Requests

Renewal requests follow the same validation and authentication procedures as a new Certificate Request and MAY re-use the information provided with the original Certificate Request, for means of verification. If for any reason re-verification fails, the certificate SHALL NOT be renewed and be subject to new key generation, in accordance with Section 6.1.1.

Renewal requests may use an existing valid certificate that has not been revoked and has the extended key use of client authentication.

4.6.4. Notification of New Certificate Issuance to Subscriber

Certificate renewals SHALL follow the same notification method as a new Certificate, in accordance with Section 4.3.2.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Certificate renewals SHALL follow the same acceptance method as a new certificate, in accordance with Section 4.4.1.

4.6.6. Publication of the Renewal Certificate by the CA

Certificate renewals SHALL follow the same publication method as a new certificate, in accordance with Section 4.4.2.

4.6.7. Notification of Certificate Issuance by the CA to other Entities

Certificate notifications to other entities SHALL follow the same entity notification method as a new certificate, in accordance with Section 4.4.3.

4.7. Certificate Re-Key

Issuing CAs SHALL treat certificate re-key requests identical to applications for new certificates and perform the same identity-proofing processes, as described in Section 3.2, and the same acceptance methods, as described in Section 4.4. Routine re-key of the issuing CA certificates SHALL be performed in accordance with the established Key Generation process of Section 6.1 in this CP.

4.8. Certificate Modification

Modification to an issued Certificate's details is not permitted. The certificate MUST first be revoked, core Subscriber information MUST remain the same (domain name, DUNS/SSN, etc.), and only inconsequential information MUST have changed (email address, phone number, etc.), before modifications to Subscriber information are allowed. The replacement certificate (i) requires a new issuance process that doesn't require the same identity and authentication procedures as a new Applicant (as in Section 4.2.1), (ii) MAY retain the same key pair, and (iii) SHALL have new validity dates.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

PIXA PKI Policy Group SHALL revoke Subscriber or Subordinate CA Certificates if one or more of the following circumstances occur:

1. Certificate revocation is requested in writing and in accordance with Section 4.9.3;
2. PIXA acquires evidence that the Certificate or key pairs were compromised or misused.
3. The Subscriber can be shown to have violated obligations under the Subscriber Agreement
4. PIXA PKI Policy Group is notified that the original Certificate request was not authorized and does not grant retroactive authorization
5. The certificate owner entity is decommissioned or end of service or end of life
6. The Issuing or Subordinate CA ceases operation for any reason and has not arranged for another CA to provide revocation support for the Certificate
7. The Issuing or Subordinate CA's right to issue Certificates has expired, is revoked or terminated, unless the CA arranged to continue maintaining the CRL/OCSP Repository
8. Any information in the certificate is inaccurate, not legally permitted, or presents an unacceptable risk to PIXA, Relying Parties, or Application Software Suppliers
9. Revocation is required per guidelines in this CP or respective CPS;
10. The Certificate was not issued in accordance with this CP, CPS or other arising factors per applicable laws or regulations.

4.9.1.1. Reasons for Revoking a Subscriber Certificate

A Subscriber Certificate SHALL be revoked within the timeframes specified in the appropriate CPS if any of the circumstances in Section 4.9.1 or additional items specified in the CA/B Forum Baseline Requirements or CA/B Forum Code Signing Baseline Requirements.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

A Subordinate CA Certificate SHALL be revoked within seven (7) days if one or more of the circumstances in Section 4.9.1 or additional items specified in the CA/B Forum Baseline Requirements or CA/B Forum Code Signing Baseline Requirements.

4.9.2. Who Can Request Revocation

Certificate revocations MAY be requested from the authorized Subscribers, RAs, or the Issuing CA. Third parties MAY also submit Certificate Problem Reports to the Issuing CA, if one or more of the circumstances in 4.9.1 occur that suggests reasonable cause to revoke the certificate.

4.9.3. Procedure for Revocation Request

The issuing CA SHALL provide Revocation Request instructions that are noted in the respective CPS to parties and maintain a 24x7 availability to accept and respond to requests by steps outlined in Section 3.4. A manual process SHALL be used to approve high assurance CA requests for Certificate revocation. Issuing CAs and/or RAs will take the appropriate actions to process the Certificate revocation, per Section 4.9.

4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within a commercially reasonable amount of time after detecting the loss or compromise of the Private Key (within 24 hours is recommended).

4.9.5. Time Within Which CA Must Process the Revocation Request

Revocation requests SHALL initiate an investigation within 24 business hours of receiving the request.

Issuing CAs and/or RAs SHALL consider whether revocation or other actions are warranted based on at least the following criteria:

1. The entity submitting the complaint;
2. The nature of the alleged problem;
3. The number of reports received about a certain Certificate or Subscriber problem; or
4. Relevant legislation.

4.9.6. Revocation Checking Requirements for Relying Parties

PIXA has no requirements for this item.

4.9.7. CRL Issuance Frequency

An Offline Root CA SHALL have a new CRL published every 6 months.

An Online Issuing CA SHALL publish a new CRL every 3.5 days.

4.9.8. Maximum Latency for CRLs

Issuing CAs SHALL ensure that the response time for CRL or OCSP requests do not exceed ten (10) seconds under normal operating conditions.

4.10. Certificate Status Service

PIXA publishes CRLs.

4.11. End of Subscription

Certificate Subscriptions end when the certificate has either been revoked or expires. PIXA PKI Policy Group will not be responsible for the recovery of expired public/private key pairs.

5. Facility, Management and Operational Controls

The CA SHALL develop, implement, and maintain a comprehensive security program which includes an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Evaluates the proficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the outcome of the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan

MUST also take into account then available technology and cost of implementing the specific measures, and SHALL implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1. Physical Security Controls

5.1.1. Site Location

CA and RA operations are conducted within physically protected environments designed to detect and prevent unauthorized use or disclosure of, or access to sensitive information and systems. The CA maintains multiple business resumption facilities for CA and RA operations. Business resumption facilities are protected with comparable physical and logical security controls. Business resumption facilities are at geographically disparate locations, so that operations MAY continue if one or more locations are disabled.

5.1.2. Physical Access

CA facilities are protected from unauthorized access, through the required use of multi-factor authentication solutions.

Facility security systems electronically log ingress and egress of authorized personnel. Physical access to cryptographic systems, hardware, and activation materials are restricted by multiple access control mechanisms, which are logged, monitored, and video recorded on a 24x7 basis.

5.1.3. Power and Air Conditioning

CA facilities are equipped with redundant power and climate control systems to ensure continuous and uninterrupted operation of CA systems.

5.1.4. Water Exposures

Commercially reasonable safeguards and recovery measures have been taken to minimize the risk of damage from water exposure.

5.1.5. Fire Prevention and Protection

Commercially reasonable fire prevention and protection measures are in place to detect and extinguish fires and prevent damage from exposure to flames or smoke.

5.1.6. Media Storage

Media containing production software, data, audit, and archival backup information SHALL be securely stored within facilities with appropriate physical and logical access controls, consistent with Sections 5.1.2 – 5.1.5, that prevent unauthorized access and provide protection from environmental hazards.

5.1.7. Waste Disposal

Sensitive waste material or PKI information SHALL be shredded and destroyed by an approved service. Removable media containing sensitive information SHALL be rendered unreadable before secure disposal. Cryptographic devices, smart cards, and other devices that may contain Private Keys or keying material SHALL be physically destroyed or zeroized in accordance with the manufacturers' waste disposal guidelines.

5.1.8. Off-Site Backup

Alternate facilities have been established for the storage and retention of PKI systems/data backups. The facilities are accessible by authorized personnel on a 24x7 basis with physical security and environmental controls comparable to those of the primary CA facility.

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted Roles consist of vetted and approved employees, contractors, or consultants that require access to or control over the CA's PKI operations. Trusted Role positions are subject to a clearly defined set of responsibilities that maintain a strict multi-person control; such that, no single person is able to perform both validation duties and certificate issuance fulfillment without a secondary review by another "trusted" team member. The personnel considered for Trusted Role positions MUST successfully pass the screening and training requirements of CPS Section 5.3. Trusted Role positions MAY include, but are not limited to, system administrators, operators, engineers, and certain executives who are designated to oversee CA operations.

5.2.2. Number of Persons Required per Task

The CA Private Key SHALL be backed up, stored, and recovered only by at least two persons in Trusted Roles using, at least, dual control in a physically secured environment.

5.2.3. Identification and Authentication for Each Role

Individuals in a trusted role position SHALL be authorized by management to perform CA duties and MUST satisfy the Personnel Controls requirements specified in Section 5.3.

5.2.4. Roles Requiring Separation of Duties

To ensure separation of duties, as described in Section 5.2.1, PKI responsibilities relating to access, operations, and audit MUST be performed by separate Trusted Roles.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

The CA verifies the identity and trustworthiness of all personnel, whether as an employee, agent, or an independent contractor, prior to the engagement of such person(s).

Any personnel occupying a Trusted Role (as defined in 5.2.1) MUST possess suitable experience and be deemed qualified. Personnel in Trusted Roles SHALL undergo training prior to performing any duties as part of that role.

5.3.2. Background Check Procedures

Prior to assignment in a Trusted Role position, the prospective CA personnel SHALL undergo and clear the necessary background checks or security screenings requirements, as required by CA hiring policies, CA/B Forum Guidelines, and local laws.

5.3.3. Training Requirements

All personnel involved with validation operations SHALL receive and pass the required training to perform the duties relative to their assigned Trusted Role. The CA SHALL retain records of the training completed by such individuals.

5.3.4. Retraining Frequency and Requirements

Trusted Role personnel SHALL receive periodic training to maintain competency with the CA's PKI-related operations and regulatory changes.

The CA SHALL maintain records of all training taken by Trusted Role personnel.

5.3.5. Job Rotation Frequency and Sequence

PIXA has no requirements for this item.

5.3.6. Sanctions for Unauthorized Actions

In accordance with the CA's HR policies, appropriate disciplinary actions SHALL be taken for unauthorized actions or other violations of PKI policies and procedures.

5.3.7. Independent Contractor Requirements

The CA MAY employ contractors, as necessary. Contractors SHALL adhere to background checks, training, skills assessment, and audit requirements, as appropriate for their role.

5.3.8. Documentation Supplied to Personnel

CA PKI personnel are required to read this CP and the respective CPS. They are also provided with PKI policies, procedures, and other documentation relevant to their job functions.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

Upon effective date, the types of events recorded SHALL be defined in the respective CPS and made available to the CA's Qualified Auditor upon request.

5.4.2. Frequency of Processing Log

Audit logs are reviewed on an as-needed basis.

5.4.3. Retention Period for Audit Log

Upon effective date, Audit logs SHALL be retained for a period defined in the respective CPS and made available to the CA's Qualified Auditor upon request.

5.4.4. Protection of Audit Log

Audit logs are protected from unauthorized viewing, modification, deletion, or other tampering using a combination of physical and logical security access controls.

5.4.5. Audit Log Backup Procedures

Audit logs are backed up and archived in accordance with business practices.

5.4.6. Audit Collection System

PIXA has no requirements for this item.

5.4.7. Notification to Event-Causing Subject

PIXA has no requirements for this item.

5.4.8. Vulnerability Assessments

The CA MUST maintain detection and prevention security controls to safeguard Certificate Systems against potential threats or vulnerabilities.

5.5. Records Archival

5.5.1. Types of Records Archived

The CA SHALL maintain archived backups of application and system data. Archived information MAY include, but are not limited to, the following:

- Audit data, as specified in Section 5.4
- Data related to Certificate requests, verifications, issuances, and revocations
- CA policies, procedures, entity agreements, compliance records,
- Cryptographic device and key life cycle information
- Systems management and change control activities

5.5.2. Retention Period for Archive

CA SHALL retain all documentation relating to a Certificate's activities for a period specified in the appropriate CPS after the Certificate ceases to be valid.

5.5.3. Protection of Archive

Archives of relevant records are secured using a combination of physical and logical access controls at both the primary and backup locations. Access is restricted to authorized personnel and SHALL be maintained for the period of time specified in Section 5.5.2.

5.5.4. Archive Backup Procedures

Adequate backup procedures SHALL be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a feasible period of time.

5.5.5. Requirements for Time-Stamping of Records

Certificates, CRLs, and other database entries SHALL contain time and date information.

5.5.6. Archive Collection System (Internal or External)

The CA SHALL employ appropriate systems for the collection and maintenance of archived records.

5.5.7. Procedures to Obtain and Verify Archive Information

Only authorized CA personnel SHALL have access to primary and backup archives. The CA MAY, at its own discretion, release specific archived information, following a formal request from a Subscriber, a Relying Party, or an authorized agent thereof.

5.6. Key Changeover

PIXA has no requirements for this item.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

All CA organizations SHALL have formal Incident Response, Disaster Recovery, and/or Business Continuity Plans that contain documented procedures to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. Business Continuity and Security Plans do not have to be publicly disclosed, but the CA SHALL make them available to auditors upon request and annually test, review, and update the procedures.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

See Section 5.7.4.

5.7.3. Entity Private Key Compromise Procedures

The CA's business continuity plan contains the procedures to address incidents in which a CA Private Key is suspected of being or has been compromised. Upon thorough investigation, appropriate actions will be taken to revoke and generate new key pairs, notify affected Subscribers, and coordinate revoking and reissuing the affected certificates.

5.7.4. Business Continuity Capabilities After a Disaster

In the event of a disaster, the CA has established and maintains business continuity capabilities to address the recovery of PKI services in the event of critical interruptions or outages with CA operations. The recovery procedures align with those identified in Section 5.7.1 and the accompanying CPS.

5.8. CA or RA Termination

In the event that it is necessary to terminate the operation of a CA, CA management will plan and coordinate the termination process with its Subscribers and Relying Parties such that the impact of the termination is minimized. The CA will make a commercially reasonable effort to provide prior notice to Subscribers and Relying Parties and preserve relevant records for a period of time deemed fit for functional and legal purposes.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. CA Key Pair Generation

The CA SHALL have effective practices and controls in place to reasonably assure that the generation of Root and Subordinate CA key pairs are performed in a physically secured environment, using cryptographic modules where appropriate that meet the requirements of Section 6.2, by multiple Trusted Role personnel, following a prepared key generation script.

6.1.1.2. RA Key Pair Generation

Where an RA requires a Enrollment Agent certificate, the CA will make all efforts to host the private key on appropriate cryptographic modules.

6.1.1.3. Subscriber Key Pair Generation

The Subscriber MAY generate their own key pairs, in accordance to the requirements set forth in Section 6.1.5 and 6.1.6. If the Subscriber does not adhere to these requirements or has a known weak Private Key, the CA SHALL reject the Certificate Request.

6.1.2. Private Key Delivery to Subscriber

If a Subscriber generates their own key pairs, Private Key delivery is not performed.

In the event the CA is authorized to generate a Private Key on behalf of a Subscriber, the Private Key will be encrypted prior to transporting to the Subscriber.

6.1.3. Public Key Delivery to Certificate Issuer

PIXA has no requirements for this item.

6.1.4. CA Public Key Delivery to Relying Parties

PIXA has no requirements for this item.

6.1.5. Key Sizes

Subscriber key length should attempt to use 4096 or equivalent sized keys. Where this is not feasible, 2048 or equivalent will be the shorted accepted. The CA must use 4096 on all Certification Authorities.

6.1.6. Public Key Parameters Generation and Quality Checking

The CA SHALL generate Private Keys using secure algorithms and parameters based on current research and industry standards.

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

Root Certificate Private Keys MUST NOT be used to sign Certificates, except in the following cases:

1. Self-signed Certificates to represent the Root CA;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates);

6.2. Private Key Protection and Cryptographic Module Engineering Controls

The CA SHALL implement physical and logical security controls to prevent the unauthorized issuance of a certificate. The CA Private Key MUST be protected outside of the validated system or device specified above, using physical security, encryption, or a combination of both, and be implemented in a manner that prevents its disclosure. The CA SHALL encrypt the Private Key with an algorithm and key-length that are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1. Cryptographic Module Standards and Controls

Online CA key pairs are generated and protected by validated FIPS 140-2 level 3 hardware cryptographic modules that meet industry standards for random number and prime number generation. The Timestamp Authority protects its signing key using a process that is at least to FIPS 140-2 Level 3, Common Criteria EAL4+ (ALC, FLR2), or higher.

Offline CA key pairs reside within the CA and SHALL remain air gapped for the duration of its lifetime. Any access to Offline key pairs must adhere to the controls described in section 6.2.2.

6.2.2. Private Key (n out of m) Multi-Person Control

The participation of multiple individuals in trusted role positions are required to perform sensitive CA Private Key operations (e.g., hardware security module (HSM) activation, signing operations, CA key backup, CA key recovery, etc.).

6.2.3. Private Key Escrow

PIXA has no requirements for this item.

6.2.4. Private Key Backup

Backup copies of CA Private Keys SHALL be backed up by multiple persons in trusted role positions and only be stored in encrypted form on cryptographic modules that meet the requirements specified in Section 6.2.1.

6.2.5. Private Key Archival

PIXA will not participate in private key archival.

6.2.6. Private Key Transfer into or from a Cryptographic Module

CA Private key transfer will only occur from one Cryptographic Module to a second Cryptographic Module based on the support lifetime or health of the module.

6.2.7. Private Key Storage on Cryptographic Module

See section 6.2.1

6.2.8. Method of Activating Private Key

Cryptographic modules used for CA Private Key protection utilize a smart card-based activation mechanism by multiple Trusted Role personnel using multi-factor authentication.

6.2.9. Method of Deactivating Private Key

PIXA has no requirements for this item.

6.2.10. Method of Destroying Private Key

CA Private Keys SHALL be destroyed when they are no longer needed or when the Certificates, to which they correspond, expire or are revoked. The destruction process SHALL be performed by multiple Trust Role personnel and documented using verifiable methods.

6.2.11. Cryptographic Module Rating

See Section 6.2.1

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Copies of CA and Subscriber certificates and Public Keys SHALL be archived in accordance with Section 5.5.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Reference relevant CPS for more requirements.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

CA SHALL protect activation data from compromise or disclosure. Appropriate cryptographic and physical access controls SHALL be implemented to prevent unauthorized use of any CA Private Key activation data.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

CA systems SHALL be secured from unauthorized access using multi-factor authentication security controls.

6.6. Life Cycle Technical Controls

PIXA has no requirements for this item.

6.7. Network Security Controls

Access to Online Certification Authorities for purposes of administration or management of the system must be strictly restricted to a designated management point.

6.8. Time Stamping

Certificates, CRLs, and other revocation database entries SHALL contain time and date information.

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

CA certificates SHALL be X.509 Version 3 format and conform to RFC 5280 standards: Internet X.509 Public Key Infrastructure Certificate and CRL profile.

7.1.1. Version Number(s)

CAs SHALL issue certificates that are compliant with X.509 Version 3.

7.1.2. Certificate Extensions

The extensions defined for the CA's X.509 v3 certificates provide methods for associating additional attributes with users or Public Keys and for managing the certification hierarchy. Each extension in a certificate is designated as either critical or non-critical.

Certificate extensions, their criticality, and cryptographic algorithm object identifiers, are provisioned according to the IETF RFC 5280 standards.

7.1.2.1. Root CA Certificate

Root CAs SHALL ensure that the content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support Name chaining, as specified in RFC 5280.

7.1.2.2. Subordinate CA Certificate

Subordinate CA Certificates MAY include extensions and values that are pertinent for their intended use, in accordance with this CP, the accompanying CPS, and as specified in RFC 5280.

7.1.2.3. Subscriber Certificate

Subscriber Certificates MAY include extensions and values that are pertinent for their intended use, in accordance with this CP, the accompanying CPS, and as specified in RFC 5280.

7.1.2.4. All Certificates

All other provisions SHALL be set in accordance with RFC 5280.

7.1.2.5. Application of RFC 5280

PIXA has no requirements for this item.

7.1.3. Algorithm Object Identifiers

PIXA has no requirements for this item.

7.1.4. Name Forms

Issuing CAs SHALL issue Certificates with Name Forms compliant with RFC 5280.

7.1.4.1. Issuer Information

PIXA has no requirements for this item.

7.1.4.2. Subject Information – Subscriber Certificates

Where certificates are not issued by the approved Registration Authorities, the OU field of the subject name SHALL have the value of the approved Service Request ticket number.

7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates

By issuing a Subordinate CA Certificate, the CA represents that it followed the procedure set forth in this CP and CPS to verify that, as of the Certificate's issuance date, all Subject Information was accurate.

7.1.5. Name Constraints

Issuing CAs reserve the right to issue Certificates with Name Constraints and mark them as critical, where necessary. Unless otherwise documented in this CP or accompanying CPS, the use of Name Constraints SHALL conform with the X.509 V3 standard (RFC 5280).

7.1.6. Certificate Policy Object Identifier

Issuer CAs MAY issue Certificates with policy identifiers set forth in Section 1.2 herein, and comply with the provisions of this CP, the respective CPS, and the CA/B Forum Baseline Requirements and CA/B Forum Code Signing Baseline Requirements.

7.2. CRL Profile

CRL Profiles comply with X.509 V3 standards.

7.3. OCSP Profile

PIXA will not be deploying OCSP and as such has no requirements on an OCSP profile.

8. Compliance Audit and Other Assessments

PIXA PKI Policy Group SHALL at all times:

1. Comply with the requirements in this CP;
2. Comply with the audit requirements set forth by PIXA, this CP and associated CPS; and

3. Be licensed as a CA in each jurisdiction of operation, where required, for the issuance of Certificates.

8.1. Frequency and Circumstances of Assessment

The CA MUST have an independent auditor annually assess the CA's compliance to the stated requirements and practices of the CP and respective CPS. The results of the audit SHALL be provided in an Audit Report indicating the compliance status with the applicable standards under the audit scheme herein.

Any changes to the CA business practices are subject to and SHALL require Self Audits, as described in Section 8.7. Any audit deficiencies SHALL be addressed and remedied, in accordance with Section 8.5. The annual audit SHALL include items mentioned in Section 8.4.

8.2. Identity/Qualifications of Assessor

The CA SHALL have an annual audit conducted by an independent licensed Auditor that demonstrates proficiency in the criteria specified in Section 8.4 and maintains a Professional Liability/Errors, & Omissions insurance policy with a minimum coverage of one million US dollars.

8.3. Assessor's Relationship to Assessed Entity

The entity that performs the scheduled audit SHALL be completely independent of the CA.

8.4. Topics Covered by Assessment

Annual audits SHALL be performed by an independent certified Auditor that assesses the CA's PKI operations in accordance with the stipulations documented in the CP and respective CPS.

8.5. Actions Taken as a Result of Deficiency

Deficiencies identified by the auditor during the compliance audit will determine the actions to be taken. The PIXA PKI Policy Group is responsible for ensuring that remediation plans are promptly developed, documented, and corrective actions are taken within an adequate timeframe corresponding to the significance of identified matters.

8.6. Communication of Results

Audit results are provided to the PIXA PKI Policy Group, who will distribute to the necessary parties, as required. General audit findings that do not impact the overall audit opinion are not required to be publicized.

8.7. Self-Audits

PIXA does not currently conduct self-audits.

9. Other Business and Legal Matters

9.1. Fees

PIXA does not charge Subscriber fees for internal certificate issuance, renewals, access and or revocation or Status Information.

9.2. Financial Responsibility

Subscribers and Relying Parties SHALL be responsible for the financial consequences to such Subscribers, Relying Parties, and to any other persons, entities, or organizations for any transactions in which such Subscribers or Relying Parties participate and which use PIXA PKI Policy Group Certificates or any services provided in respect to such Certificates. PIXA PKI Policy Group makes no representations and gives no warranties or conditions regarding the financial efficacy of any transaction completed utilizing a Certificate provided by PIXA PKI Policy Group or any services provided in respect to such Certificates and neither PIXA nor any of its subcontractors, distributors, agents, suppliers, employees, or directors SHALL have any liability except as explicitly set forth herein in respect to the use of or reliance on any such Certificate or any services provided in respect to such a Certificate.

9.2.1. Insurance Coverage

Any insurance requirements fall under PIXA existing general liability and professional liability insurance and existing policy limits.

9.3. Confidentiality of Business Information

Each CA will have appropriate terms and policies in place to maintain the confidentiality and privacy of applicable information and, at the same time, publish such information as is necessary for proper operation of each PKI service.

9.4. Privacy of Personal Information

All information gathered by PIXA PKI Policy Group in the management of the CA is owned by PIXA. No individual Personally Identifiable Information should be used in the issuance of certificates, and where such is found, should be identified and acted upon pursuant to PIXA privacy policies.

9.5. Intellectual Property Rights

The following are the property of PIXA:

- This CP;
- Policies and procedures supporting the operation of PIXA PKI Policy Group;
- Certificates and CRLs issued by PIXA PKI Policy Group managed CAs;
- Distinguished Names (DNs) used to represent entities within the PIXA PKI Policy Group CA hierarchy; and
- CA infrastructure and Subscriber key pairs.

This Certificate Policy (CP) incorporates material derived from the *Microsoft PKI Services Certificate Policy (CP)* Version 3.1.9, published April 21, 2025. The Microsoft document is licensed under the Creative Commons Attribution–NoDerivatives 4.0 International License (CC BY-ND 4.0). PIXA retains all intellectual property rights in and to this adapted CP, which is specific to PIXA and includes additional original material.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement for the Certificate;

2. All Relying Parties who reasonably rely on a Valid Certificate. PIXA PKI Policy Group represents and warrants to the Certificate Beneficiaries, during the period when the Certificate is valid, the CA has complied, in all material aspects and to the best of its knowledge with the CP or CPS in issuing and managing the Certificate.

The certificate warranties specifically include the following:

1. Right to Use Domain Name or IP Address: That, at the time of issuance, PIXA PKI Policy Group
   a. implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Service Name, Domain, and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);
   b. followed the procedure when issuing the Certificate; and
   c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
2. Authorization for Certificate: That, at the time of issuance, PIXA PKI Policy Group
   a. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
   b. followed the procedure when issuing the Certificate; and
   c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
3. Accuracy of Information: That, at the time of issuance, PIXA PKI Policy Group
   a. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate;
   b. followed the procedure when issuing the Certificate; and c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
4. Identity of Applicant: That, if the Certificate contains Subject Identity Information, PIXA PKI Policy Group
   a. implemented a procedure to verify the identity of the Applicant in accordance with the CP/CPS Section 3.2 and CP/CPS Section 7.1.4.2.2;
   b. followed the procedure when issuing the Certificate; and
   c. accurately described the procedure in the CA's Certificate Policy or Certification Practice Statement;
5. Subscriber Agreement: That, if PIXA PKI Policy Group and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable

Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Subscriber Agreement/Terms of Use;

6. Status: That PIXA PKI Policy Group maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (revoked) of all unexpired Certificates; and
7. Revocation: That the CA will revoke the Certificate for any of the reasons specified in this CP or accompanying CPS, but only to the extent the CA gains actual, undisputed knowledge that one of these reasons has arisen.

The foregoing representations and warranties regarding procedures relate solely to facts surrounding the establishment and documentation of the procedures and that PIXA PKI Policy Group followed them. They expressly do not relate to, and PIXA PKI Policy Group expressly disclaim any representations and warranties regarding, the outcome or results of having followed such procedures.

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with the CP and associated CPS, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA where the Subordinate CA issuing the Certificates.

9.6.2. RA Representations and Warranties

PIXA authorizes its on premises Microsoft Active Directory Domain Services and Entra ID (via InTune and NDES) to act as Registration Authorities.

9.6.3. Subscriber Representation and Warranties

PIXA PKI Policy Group SHALL require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or

2. The Applicant's acknowledgement of the Terms of Use.

PIXA PKI Policy Group SHALL implement a process to ensure that each Subscriber Agreement or Terms of Use is enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request.

PIXA PKI Policy Group MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
5. Reporting and Revocation: An obligation and warranty to:
   (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
   (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.

6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. Responsiveness: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.7. Disclaimers of Warranties

Except for express warranties stated in this CP, the CA disclaims all other warranties, promises and other obligations (express, implied, statutory, or otherwise). In addition, and without limiting the foregoing the CA is not liable for any loss:

- To CA or RA services due to war, natural disasters or other uncontrollable forces;
- Incurred between the time a Certificate is revoked and the next scheduled issuance of a CRL;
- Due to unauthorized use of Certificates issued by the CA, or use of Certificates beyond the prescribed use defined by this CP;
- Arising from the negligent or fraudulent use of Certificates or CRLs issued by the CA; and
- Due to disclosure of personal information contained within Certificates or CRLs.

9.8. Limitations of Liability

For delegated tasks, PIXA PKI Policy Group and any Delegated Third-Party MAY allocate liability between themselves contractually as they determine, but PIXA PKI Policy Group SHALL remain fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated.

If PIXA PKI Policy Group has issued and managed the Certificate in compliance with its Certificate Policy and Certification Practice Statement, PIXA PKI Policy Group MAY disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's Certificate Policy and Certification Practice Statement. If PIXA PKI Policy Group has not issued or managed the Certificate in compliance with these Requirements and its Certificate Policy

and Certification Practice Statement, PIXA PKI Policy Group MAY seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that PIXA PKI Policy Group desires. If PIXA PKI Policy Group chooses to limit its liability for Certificates that are not issued or managed in compliance with its Certificate Policy and Certification Practice Statement, then PIXA PKI Policy Group SHALL include the limitations on liability in the CA's Certificate Policy or Certification Practice Statement.

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE A CERTIFICATE, INCLUDING AS A RESULT OF (I) ANY TERMINATION OR SUSPENSION OF THIS AGREEMENT OR THE CPS OR REVOCATION OF A CERTIFICATE, (II) OUR DISCONTINUATION OF ANY OR ALL SERVICE OFFERINGS IN CONNECTION WITH THIS AGREEMENT, OR, (III) ANY DOWNTIME OF ALL OR A PORTION OF CERTIFICATE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE CONTENT OF ANY CERTIFICATE (INCLUDING ANY ALLEGEDLY ERRONEOUS CONTENT) OR YOUR RELIANCE ON SUCH CONTENT; (C) THE PROCESS OF ISSUING, REPORTING THE STATUS OF, OR REVOKING ANY CERTIFICATE (INCLUDING ANY ALLEGEDLY FLAWED PROCESS) OR YOUR RELIANCE ON SUCH PROCESS; (D) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (E) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO MICROSOFT'S CERTIFICATE SERVICES; OR (F) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, MICROSOFT AND ITS AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY IN CONNECTION WITH THIS AGREEMENT AND ALL CERTIFICATES ISSUED HEREUNDER, IS LIMITED TO DIRECT DAMAGES INCURRED IN REASONABLE RELIANCE IN AN AMOUNT NOT EXCEEDING THE LESSER OF THE AMOUNT PAID BY YOU FOR THE CERTIFICATE(S) AT ISSUE OR THE AMOUNTS PAID FOR THE CERTIFICATE SERVICES FOR THE CERTIFICATE(S) AT ISSUE IN THE LAST TWELVE (12) MONTHS BEFORE THE CLAIM AROSE (UNLESS THE FOREGOING AMOUNT IS ZERO, IN WHICH CASE SUCH DIRECT DAMAGES LIMIT WILL BE DEEMED TO BE FIVE U.S. DOLLARS).

9.9. Indemnities

Subscribers to PIXA PKI Policy Group PKI do not assume any obligation or potential liability of the CA.

9.10. Term and Termination

9.10.1. Term

This CP becomes effective upon publication in the Repository.

This CP, as amended from time to time, SHALL remain in force until it is replaced by a new version. Amendments to this CP become effective upon publication in Repository.

9.10.2. Termination

This CP and any amendments remain in effect until replaced by a new version.

9.11. Individual Notices and Communications with Participants

PIXA accepts notices related to this CP at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from PIXA. If an acknowledgement of receipt is not received within five days, the sender MUST resend the notice in Service Request form. PIXA MAY allow other forms of notice in its Subscriber Agreements.

9.12. Amendments

9.12.1. Procedure for Amendment

Amendments to this CP MAY be made by the PIXA and SHALL be approved by the PIXA PKI Policy Group, as per Section 1.5.4.

9.13. Dispute Resolution Provisions

In the event of any dispute involving the services or provisions covered by this CP, the aggrieved party SHALL notify a member of PIXA PKI Policy Group regarding the dispute.

PIXA PKI Policy Authority will involve the appropriate PIXA personnel to resolve the dispute.

9.14. Governing Law

The Laws of PIXA govern the interpretation, construction and enforcement of this CP.

9.15. Compliance With Applicable Law

See section 9.14

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

PIXA has no requirements.

9.16.2. Assignment

PIXA has no requirements.

9.16.3. Severability

In the event of a conflict between this CP or accompanying CPS and a law, regulation, or government order (hereinafter 'Law') of any jurisdiction in which PIXA PKI Policy Group operates or issues certificates, PIXA PKI Policy Group MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law.

In such an event, PIXA PKI Policy Group SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of PIXA PKI Policy Group's CPS or CP a detailed reference to the Law requiring a modification of CP or CPS implemented by PIXA PKI Policy Group.

PIXA PKI Policy Group MUST also (prior to issuing a certificate under the modified requirement) PIXA of the relevant information newly added to its CPS or CP by sending a message to the PIXA governing body.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice,

modification to PIXA PKI Policy Group's CPS or CP, and a notice to the PIXA governing body must be made within 90 days.