INFO TECH - CP/CPS V1.0

INFO TECH, INC. CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

VERSION 1.0

Info Tech, Inc.
5700 SW 34th St. Suite 1235
Gainesville, FL 32608

January 18, 2016

CONTENTS

1. INTRODUCTION

1.1 Overview

This Certificate Policy and Certification Practice Statement (herein referred to as the "Policy" or as the "CP/CPS," as appropriate) specifies minimum requirements for the issuance and management of digital certificates that shall be used in authenticating actions of users accessing resources of the Info Tech, Inc. (herein referred to as "Info Tech") and the resources of other entities (relying parties) which accept those certificates. This CP/CPS is issued and administered under the authority of the Info Tech Executive Team via the Info Tech Information Security Review Board ("ISRB"), Legal Department, Information Technology ("IT") Department, and Human Resources ("HR") Department. For clarification of any aspect of this CP/CPS contact legal@infotechfl.com.

Info Tech acts as the Root CA for several different classes of digital certificates, which are described later in this CP/CPS. It is expected that relying parties will generally trust all Info Tech certificates, though a relying party may choose to trust any class of Info Tech certificate separately. Any software or repository used to distribute and authenticate policies, certificates and the like are referred to as the "Info Tech PKI."

This document illustrates the policies and practices that govern the Info Tech PKI. The Info Tech PKI is integrated with the Info Tech user database, Info Tech Express, and other applicable identity management systems. Various methods are used to enroll users in the Info Tech user database, create user accounts for them, and assign them a distinguished name.

To obtain credentials, Info Tech PKI subscribers complete one of a small variety of processes which are either web-based or software-based. Upon completion of the applicable process, Info Tech-PKI generates a subscriber's private key on the subscriber's local host machine and a request for approval pending authentication and verification by Info Tech PKI. If the request is authenticated and verified according to the standard of verification corresponding to the class of Info Tech PKI certificate applied for, the subscriber receives a signed certificate from Info Tech.

1.2 Document Name and Identification

Document title: [Info Tech CP/CPS] Info Tech, Inc. Certificate Policy and Certification Practice Statement
This Policy is published at: https://ca.infotechexpress.com.
Document version: 0.1
Document Date: May 27, 2015 12:00 AM EST
OID: N/A

1.3 PKI Participants

1.3.1 Certification Authority

This policy is valid for the CA Info Tech PKI. CA Info Tech PKI will only sign end-entity certificates. There are no subordinate CAs.

1.3.2 Registration Authorities

Trained Info Tech certification staff serve as RAs for the Info Tech PKI. This trained certification staff performs verification and authentication functions which are not performed via automated process within the Info Tech PKI. Roles and responsibilities of the trained certification staff are enumerated *infra*.

1.3.3 Subscribers (End Entities)

Subscribers who receive X.509 certificates verified and authenticated via Info Tech PKI systems and software may be individuals, individuals acting as agents of nonperson (corporate) entities, or both. These certificates may be used for the purpose of authentication, encryption, and digital signing by those individuals to whom the certificates have been issued.

1.3.4 Relying Parties

Any party using or employing any Info Tech system or software may accept certificates issued by Info Tech PKI. A party *not* using any Info Tech system or software may always accept certificates issued by Info Tech PKI if they have agreed to an Info Tech PKI Relying Parties Agreement or other express agreement with Info Tech. In the absence of such agreement and aside from use within the Info Tech systems or software, Info Tech neither authorizes nor guarantees certificates issued by Info Tech PKI to be accepted by any party, however, such parties may choose to accept certificates issued by Info Tech PKI at their sole risk and discretion.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Info Tech PKI issued X.509 certificates which have been approved for use by trained Info Tech certification staff, are not expired, and have not been revoked may be used for the purpose of authentication, encryption, and digital signing within Info Tech systems or software, or for other uses expressly approved by agreement with Info Tech.

1.4.2 Prohibited Certificate Uses

Other uses of Info Tech PKI issued X.509 certificates are not prohibited, but neither are they supported or guaranteed by Info Tech in any way whatsoever. Such uses are at the sole risk of the user of the certificate and the party seeking to rely upon the certificate.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP/CPS is administered by Info Tech, Inc.

1.5.2 Contact Person

The point of contact for this CP/CPS and matters related to this CP/CPS is:

Info Tech Legal Dept.
Phone number: (352) 381-4400
Postal address: 1235 SW 34th Street, Suite 1235, Gainesville, FL 32608
Email address: legal@infotechfl.com.

1.5.3 Person Determining CPS Suitability for the Policy

The Info Tech Executive Team is ultimately responsible for determining the suitability of this CP/CPS.

1.5.4 CPS approval procedures

Any policy changes to this CP/CPS require approval by the Info Tech Executive Team or duly appointed designees thereof. Appointed designees, if any, are listed here along with the scope of authority delegated by the Info Tech Executive Team.

DESIGNEES: N/A.

1.6 Definitions and Acronyms

CA Certificate: Info Tech CA certificates can be one of two types: the **Root Certificate** is a certificate self-signed by Info Tech. The root certificate is used to sign Info Tech **Intermediate Certificates**. Intermediate certificates are the certificates which are used to sign end user certificates issued according to the terms and conditions of this CP/CPS.

Certificate Authority (CA): an authority trusted by one or more users and relying parties to create and assign public key certificates.

Certificate Policy and Certification Practice Statement (CP/CPS): a named set of rules and statement of practices that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. The CP/CPS is referred to by relying parties to determine the level of trust to be assigned to any class of certificates issued properly according to the policies and procedures stated in the CP/CPS, including any warranties and representations made by the CA and any entity operating within the CP/CPS web of trust.

Certificate Revocation List (CRL): a CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made freely available in a public repository.

Info Tech PKI: the Info Tech, Inc. Public Key Infrastructure system, for which Info Tech acts as the sole CA and provides the methods of issuance of digital certificates, as well as certain non-exclusive methods for public/private key generation for subscribers.

Public Key Infrastructure (PKI): the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke digital certificates based on public-key cryptography.

Registration Authority (RA): an entity that is responsible for identification and authentication of certificate subjects (subscribers), but that does not sign or issue certificates. The Info Tech PKI does not employ any subordinate RA and performs all subject authentication and verification according to the terms of this CP/CPS.

Relying Party: a recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Subscriber: a person (an individual) that has been issued an Info Tech PKI digital certificate according to the terms of this CP/CPS.

User: one who accesses any portion of the Info Tech PKI system, network, or other Info Tech system or network. As applicable, this may be a subscriber, an Info Tech employee, or a relying party; usage in this document should be determined by context in each case.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Info Tech PKI will maintain a repository at https://ca.infotechexpress.com

2.2 Publication of Certification Information

This repository will contain:

- Self-signed certificates for the Info Tech PKI
- CRLs for the Info Tech PKI
- General information about the Info Tech PKI, including postal address and contact email address.
- The most recent and historical copies of all Certificate Policies for the Info Tech PKI, including this Policy.

2.3 Time or Frequency of Publication

All CRLs will be published on any day on which the CRL is updated. A CRL is deemed current until an updated version is published.

This CP/CPS shall be published immediately following any update.

2.4 Access Controls on Repositories

Access to the repository for modification is restricted to Info Tech staff duly assigned with the role or responsibility of modification of the repository. See *infra* for details regarding Info Tech PKI procedural controls.

Read access to the repository (via HTTP or HTTPS) is unrestricted. The repository is publicly available for read access. Best effort subject to existing Info Tech policy and Info Tech business judgment will be provided to maintain the availability of the repository 24x7.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Common name, organization, and country names will always be used. Other names may be used if needed.

3.1.2 Need for Names to be Meaningful

Names are neither meaningful nor strictly serial in nature.

3.1.3 Anonymity or Pseudonymity of Subscribers

Subscribers may not remain anonymous or pseudonymous.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

Each subject name issued by Info Tech PKI will be issued to one and only one individual as identified by a record in the user database. The user database management system implements checks to ensure the uniqueness of assigned distinguished names. User records are never purged from the database or reused, to ensure that distinguished names will never be assigned to another individual.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Certificate requests must be digitally signed by the private key associated with the public key in the request using a process that is run by the user on the client side of the request. Whether the process is client- or server-side is dependent on the method of application for (not the type of) the certificate.

3.2.2 Authentication of Organization Identity

- STANDARD CERTIFICATE: Organization Identity shall be authenticated by verification of organization legal name via state, federal, or public registry, typically the Secretary of State online repository for a given state.

- NONSTANDARD CERTIFICATE: Organization Identity may be verified in the same manner as an Organization Identity is verified for a Standard Certificate, however, if an organization is not required to be registered via any state, federal, or public registry, the Organization Identity shall be verified via other reasonable and verifiable means. This type of verification is escalated to the Info Tech Legal Department, and all such verifications shall be logged, specifically listing the means used to verify the Organization Identity.

3.2.3 Authentication of Individual Identity

- STANDARD CERTIFICATE: Individual Identity shall be verified via a three-part verification process. Part one: the applicant must demonstrate the capability to send and receive email at an email address provided by the applicant. Part two: the applicant must provide an image of a state or federal government issued identification which includes a photograph of the applicant. Types of identification accepted for a Standard Certificate are: Driver's License, State-Issued ID Card, and Passport. Part three: the applicant must verbally verify that the applicant is in fact applying for the Info Tech certificate via a telephone conversation with trained Info Tech personnel. The telephone number used for verbal verification is provided by the applicant and may be verified via independent means. Information sufficient to confirm the possession of the identification provided to Info Tech during Part two and information sufficient to confirm control of the email address provided during Part one of the Authentication of Individual Identity procedure may also be verified during the verbal verification portion of the Authentication of Individual Identity.
- NONSTANDARD CERTIFICATE: Authentication of Individual Identity shall be verified in the same manner as Authentication of Identity is verified for a Standard Certificate, except that state or government identification *other than* Driver's License, State-Issued ID Card, or Passport will be reviewed. Any identification reviewed under this standard shall contain a photograph of the applicant, must be issued by a state or federal government agency, must contain additional identifying information about the applicant, and must be a document of the type that would reasonably be considered to suffice for identification of the applicant for other identity verification purposes. This type of verification is escalated to the Info Tech Legal Department, and all such verifications shall be logged, specifically listing the means used to approve the acceptability of the identification used for Authentication of Individual Identity. Other requirements for Authentication of Individual Identity identified above for a Standard Certificate (demonstration of the capability to send and receive email at an email address provided by the applicant, verbal verification of the applicant's intent to apply for the Info Tech certificate) shall still apply and may not be omitted for a Nonstandard Certificate.

3.2.4 Non-Verified Subscriber Information

During the application process for an Info Tech PKI certificate, or before the application process, Info Tech may come to be in possession of certain kinds of an applicant's personal information which are not verified - or, if verbally verified with the applicant but not required to be logged - as part of the certificate application process, as such verification would be either irrelevant or redundant. This information may or may not be included on the certificate. This type of information may include, without limitation:

- Applicant's home address, ID serial number, SSN, or other information which may be present on an image of an identification document or other document provided by the applicant. [Not relevant to use of certificate]
- Organization address. [Not relevant to use of certificate]

- Organization telephone number or telephone number of applicant. [Not relevant to level of trust assigned to the certificate]

Documentation provided by the applicant during the application process, including any images of identification provided by the applicant, is securely deleted upon approval or ultimate rejection of the application.

3.2.5 Validation of Authority

Applicants requesting Info Tech PKI certificates must be authenticated as the applicant identified in the certificate. Applicants certify as part of the application process that the applicant as an individual has the authority to act on behalf of and bind the organization that the applicant professes to represent, whether as employee, owner, or agent. This certification is a contractual matter between Info Tech and the subscriber. Relying parties should take note that this contractual validation is not intended to replace any process or requirement of the relying party for validation of authority (such as approved vendor lists, owner or officer requirements, or the like).

3.2.6 Criteria for Interoperation

- STANDARD CERTIFICATES: Info Tech permits interoperation within any Info Tech system or software. Info Tech permits interoperation outside of Info Tech systems or software if the interoperation is the natural business result of a performance pursuant to or related to an executed Relying Parties Agreement or other express agreement which implies interoperability. Info Tech is otherwise under no obligation to ensure interoperability of Info Tech PKI certificates to any entity whatsoever.
- NONSTANDARD CERTIFICATES: These criteria are the same as the criteria for Standard Certificates, however, in certain instances, Relying Parties may have the ability to accept Standard Certificates but to refuse Nonstandard Certificates as a class (but not on an individual certificate basis).

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Info Tech shall verify Subscriber's possession of the Subscriber's private key by any acceptable means prior to execution of a routine re-key procedure by Info Tech.

3.3.2 Identification and Authentication for Re-Key after Revocation

No certificate shall be re-keyed after revocation.

3.4 Identification and Authentication for Revocation Request

Subscribers may request revocation by contacting Info Tech via email or telephone. Parties other than subscribers may request revocation of a subscriber's certificate only if they can sufficiently prove the compromise of that subscriber's certificate or that the certificate is no longer controlled by that subscriber.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can Submit a Certificate Application

Any user granted an Info Tech Express user account may submit an application for an Info Tech PKI certificate.

4.1.2 Enrollment Process and Responsibilities

Applicant is responsible for providing required information to be authenticated (such as legal name, organization legal name, identifying documents), is required to click/accept the Subscriber Agreement, and is required to verbally verify that all information provided to Info Tech for the purpose of issuing a certificate to the Applicant is true and correct.

Info Tech trained personnel are responsible for review and authentication of information provided by the applicant, contacting the applicant to obtain verbal verification of the applicant's intent to obtain an Info Tech certificate, and for affirmatively approving or rejecting an application.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Info Tech authenticates all certificate requests as described in 4.1 *supra*. Electronic communications between the subscriber, Info Tech PKI, and the user database are encrypted with industry-standard methods to protect the chain of trust during application processing. Within the Info Tech PKI, the chain of trust is protected by the secured process of translation from an authenticated certificate signing request to delivery of a signed certificate.

4.2.2 Approval or Rejection of Certificate Applications

All certificate applications that meet all criteria for acceptance and are authenticated according to all controls and protocols will be manually approved by trained Info Tech certification staff. Certificate applications that do not meet each and every criteria for acceptance or do not pass all controls and protocols for authentication for the corresponding class of certificate will be rejected.

4.2.3 Time to Process Certificate Applications

The time to process any given certificate application varies, depending on the type of certificate, the authentication and verification protocols required for that certificate, the volume of certificate requests, and business operating hours. Certificate applications and related authentication and verification procedures are only processed during regular Info Tech business hours. Verbal verification for subscribers

can only be performed if the subscriber is available and answers Info Tech's telephone call to the applicant for the purpose of verbal verification.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Certificate applications are authenticated and verified after and only after a complete certificate application has been submitted to the Info Tech PKI. After and only after all authentication and verification has been successfully performed, Info Tech certification staff shall immediately authorize issuance and disbursement of a certificate.

All actions, including rejections, associated with Info Tech PKI certificate applications are either automatically or manually logged electronically by Info Tech certification staff and the Info Tech PKI system.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Subscribers will be notified of the issuance of any certificate electronically via email. Info Tech certification staff will also notify the subscriber verbally that the certificate is authorized for issue at the end of the successful verbal verification.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Certificate acceptance is assumed due to the specific actions taken to accept the terms of the certificate electronically, request the certificate, pay any associated fees, and provide any associated documentation and verbal verification prior to certificate issue.

4.4.2 Publication of the Certificate by the CA

Certificates are constructively published upon issue by Info Tech.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No notification to other entities will be provided.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must:

- Exercise due care to protect the integrity of the private key corresponding to their certificate, including:
    - Never removing or compromising the encryption measures designed to protect the security of the private key;

    - Never sharing the private key between people; and
    - Promptly notifying Info Tech of any incident which may involve a possibility of exposure of a private key.
- Observe any restrictions on private key and certificate use.
- Not represent that their certificate is guaranteed by Info Tech for trust to any entity that is not relying upon that certificate within the normal use of Info Tech systems or software, is not a party to an Info Tech PKI Relying Party Agreement, or is not party to another express agreement to rely on Info Tech PKI certificates.
- Use the certificate in a manner consistent with the designed use of the certificate.
- Only use the certificate if the certificate is accepted by the subscriber and authorized for the subscriber's use by Info Tech.
- Discontinue use of the certificate if it has been revoked or has expired.

Subscribers are notified of these and other responsibilities:

- Via notice accessible from a relevant Info Tech website;
- Via acknowledgement of the terms of use and the subscriber agreement during the submission process of an application for an Info Tech PKI certificate; and
- Via this document, which is available in the Info Tech PKI repository and the Info Tech corporate website.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties should:

- Review the provisions of this Info Tech PKI CP/CPS and any Relying Party Agreement or other express agreement for which the relying party is in privity of contract with Info Tech.
- Verify any Nonstandard Certificates to their own satisfaction via any method of their own choosing.
- Checking any Info Tech PKI certificate against all published Info Tech PKI repository CRLs.
- Not presume authorization of an end entity based solely on possession of an Info Tech PKI certificate or its corresponding private key.
- Observe restrictions on private key and certificate use.

Relying parties are notified of these and other guidelines:

- Via notice accessible from a relevant Info Tech website;
- Via notice of this document's incorporation into any Relying Party Agreement or any other express agreement; and
- Via this document, which is available in the Info Tech PKI repository and the Info Tech corporate website.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Info Tech PKI X.509 certificates are renewed automatically prior to expiration unless they have been revoked or the Subscriber no longer has an account or subscription associated with an Info Tech service.

4.6.2 Who May Request Renewal

Subscribers may request renewal; a renewal request is assumed unless a subscriber indicates the intent to revoke the Subscriber's certificate.

4.6.3 Processing Certificate Renewal Requests

This process is automatic and happens within the Info Tech PKI CA system.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

Acceptance is implied by not requesting revocation; is expressly confirmed by use of the certificate.

4.6.6 Publication of the renewal certificate by the CA

Publication takes place in the same manner as the publication of a new certificate.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-Key

Info Tech shall be the sole entity which determines the need for a re-key event.

4.7.2 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.3 Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation.

4.7.4 Publication of the Re-Keyed Certificate by the CA

No stipulation.

4.7.5 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Info Tech PKI X.509 certificates are not modified. Subscribers may apply for a new certificate via the normal application procedure.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificates issued by the Info Tech PKI will be revoked in any of the following circumstances:

- The private key is suspected or reported to be lost or exposed.
- The information in the certificate is believed to be, or has become inaccurate.
- The certificate is reported to no longer be needed.
- Info Tech may revoke any certificate for any reason and at Info Tech's sole discretion.

4.9.2 Who can Request Revocation

Info Tech Legal, Directors and Officers may request revocation of any certificate issued by Info Tech PKI.

The subscriber may request revocation.

Entities other than the subscriber who suspect a certificate issued by the Info Tech PKI may be compromised should contact Info Tech Legal.

4.9.3 Procedure for Revocation Request

Subscribers should request revocation via the methods described in 3.4 *supra*.

Non-Info Tech, non-subscriber entities should send requests for revocation via email to legal@infotechfl.com.

Info Tech Legal, Directors and Officers may request revocation of any Info Tech PKI certificate orally or in writing to qualified Info Tech certification staff.

4.9.4 Revocation Request Grace Period

There shall be no grace period during which a certificate may be revived from a revoked status. A subscriber must request a new certificate to replace the subscriber's revoked certificate.

4.9.5 Time Within which CA Must Process the Revocation Request

Requests must be processed within one business day of the request *unless* the request is based solely on the report of a non-subscriber, non-Info Tech entity. In such cases, requests will be investigated by Info Tech Legal by whatever means are available and appropriate; however, in no case will an investigation by Legal take more than two business days. After the Legal investigation is concluded, Legal must immediately either render a decision to revoke the certificate or to disregard the request. All requests for revocation which result in a Legal Department investigation are logged, along with the findings and result of the investigations.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties are advised to obtain and consult a valid CRL from https://ca.infotechexpress.com/crl

4.9.7 CRL Issuance Frequency

CRLs will be published at least daily on any day in which a revocation of an Info Tech PKI certificate takes place.

4.9.8 Maximum Latency for CRLs

One business day.

4.9.9 Circumstances for Suspension

There is no suspension status for Info Tech PKI X.509 certificates. The certificates, once authorized and issued, are either authorized, expired, or revoked.

4.10 Certificate Status Services

N/A

4.11 End of Subscription

Subscribers may terminate their subscription as described in 3.4 *supra*.

4.12 Key Escrow and Recovery

Info Tech does not escrow and cannot recover Info Tech PKI X.509 certificate private keys. The subscriber is responsible for any backup mechanism for his or her own private keys.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

The physical site housing all data required to manage the certificate life-cycle is in the United States.

5.1.2 Cloud Vendor

All applicable services required to manage the certificate life-cycle the tasks are hosted by a cloud vendor in a suitable cloud environment. The vendor must be verified to meet the following standards:

Certifications:

- PCI 3.1
- ISO 27001/27017 - Information Security Management

Standards Reports:

- Service Organizational Controls (SOC) 1, Type II - Effective operational and data safeguarding controls
- SOC 2, Type 2/SOC 3 - Effective security and availability controls

The vendor is audited for compliance annually.

5.1.3 Off-Site Backup

Backups are retained within the cloud vendor at a separate physical location.

5.2 Procedural Controls

5.2.1 Trusted Roles

Persons acting in trusted roles for the Info Tech PKI are trained Info Tech certification staff, internal auditors, and system administration personnel. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security or trustworthiness of the Info Tech PKI operations.

5.2.2 Number of Persons Required per Task

Each task identified in 5.2.4 *infra* may require one or more persons acting in a trusted role, however, no person authorized to perform one or more tasks of any of the three sets of functions listed in 5.2.4 *infra* may perform a task listed within one of the two other sets of functions.

5.2.3 Identification and Authentication for Each Role

All trusted role personnel are required to authenticate themselves before they are allowed access to systems necessary for them to perform their trusted roles.

5.2.4 Roles Requiring Separation of Duties

The following duties are assigned to those persons in trusted roles:

- Authorization functions such as verification of information in subscriber certificate applications and approvals of subscriber certificate applications and revocation requests: issuing and revoking subscriber certificates, identity verification, compliance with issuance and revocation steps such as managing the certificate request queue and completing certificate approval checklists [Info Tech certification staff],
- Audit, review, and oversight functions: reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits [internal auditors],
- Info Tech PKI key management and Info Tech PKI administration functions: installs and configures CA software including key generation, key backup, and key management; installs and configures system hardware, including servers, routers, firewalls, and network configurations [Info Tech PKI system administration].

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Info Tech is responsible and accountable for Info Tech PKI operations and ensures compliance with this Info Tech CP/CPS. Info Tech's personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and the satisfactory performance of their duties. All trusted role personnel are citizens of the United States or are authorized to work in the United States.

Management and operational support personnel involved with Info Tech PKI operations possess experience with information security and risk assessment, knowledge of PKI and digital signature technology, and training in Info Tech security policies including policies regarding the stewardship of personal information of individuals. Info Tech ensures that all individuals assigned to Info Tech PKI trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CP/CPS.

5.3.2 Background Check Procedures

Info Tech performs the following background checks prior to extending a job offer to any person:

- Verification of identity via government-issued documents
- Verification of citizenship or of legal ability to work in the U.S. (e-Verify)
- Criminal background check
- Credit check

Human Resources makes an adjudication decision, with the assistance of Legal when necessary, as to whether the individual is suitable for the position to which they were assigned.

5.3.3 Training Requirements

Info Tech requires all employees to attend training on data security and personal information security upon hire and then requires annual in-person retraining on those same policies.

Employees assigned to Info Tech PKI trusted roles receive the following additional training:

- basic PKI knowledge,
- Info Tech PKI software and systems used by Info Tech,
- authentication and verification policies and procedures,
- common threats to the validation process (identity fraud, phishing and social engineering, etc).
- applicable industry and government guidelines.

This Info Tech PKI trusted role training is provided by a combination of internal experts and mentors. Info Tech maintains records of training and what types of training was completed. Info Tech certification staff must have the minimum skills necessary to perform their validation duties and must pass an internal examination before they are permitted to perform their trusted roles.

5.3.4 Retraining Frequency and Requirements

Retraining takes place throughout an employee's period of hire as part of a program of continuing education. Although there is no set schedule for retraining, each trusted role employee must participate in a retraining workshop yearly and must also annually pass an internal examination. If the internal examination for a trusted role employee is not passed satisfactorily, that employee will be removed from the trusted role and may be assigned to other duties until satisfactory performance on the examination can be demonstrated.

5.3.5 Job Rotation Frequency and Sequence

N/A

5.3.6 Sanctions for Unauthorized Actions

Trusted role employees failing to comply with this CP/CPS, knowingly or negligently, are subject to administrative or disciplinary actions including termination of employment or criminal sanctions. If cited for unauthorized, inappropriate, or illegal actions, the employee will immediately be removed from the trusted role pending investigation and review. After review and discussion with the employee of the unauthorized action, the employee may be subject to any sanction up to and including termination.

5.3.7 Independent Contractor Requirements

Info Tech does not permit independent contractors to perform trusted roles.

5.3.8 Documentation Supplied to Personnel

Employees in trusted roles are provided with all documentation necessary for them to perform their duties, including this CP/CPS, Internal Controls documentation, Information Security Program documentation, identity verification and authentication policies and procedures, and other information.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

All Info Tech systems require authentication and identification at system logon, whether the system is internal or external, and whether it is being accessed as an employee or an end-user non-employee. Important system actions are logged to establish the accountability of the operators who initiate such actions. Logging is automatic and actions which require urgent notice are reviewed immediately. For each event, Info Tech records the relevant: date and time, type of event; success or failure; and user or system that caused the event or initiated the action. All event records are available to auditors as proof of Info Tech's practices.

AUDITABLE EVENTS:

SECURITY AUDIT
Any changes to the audit parameters or matrices
Any attempt to delete or modify the logs
Any security-relevant changes to the configuration of any Info Tech PKI system component
Installation of any Info Tech PKI or other software, patches
Installation or removal of any hardware security component
System startup
Backup or restoration of the CA database
Any access to the CA database
Any use of any root private key

AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to log in to a given system
Number of authentication attempts that occur during login
Administrator unlocks an account that had been locked as a result of unsuccessful authentication attempts
Logon attempts to administrator accounts for Info Tech PKI software

DATA ENTRY / EXPORT
All security-relevant data that is entered in the system
All security relevant messages that are received by the system
All successful and unsuccessful requests for confidential and security-relevant information

CERTIFICATE EVENTS
All certificate requests, including issue, modification, and revocation
All status changes (authorized, revoked, expired)
Certificate issuance
Verification activities
All changes to the certificate profile
All changes to the revocation profile
All changes to the CRL profile
Generation of CRLs

ACCOUNT ADMINISTRATION
Roles and users are added or deleted
Access control privileges of an account or role is modified
Appointment of an individual to a trusted role
Attempts to set or change a password

SYSTEM ERRORS, WARNINGS, CRASHES

Crashes / hardware or equipment failures, power outages
Software error conditions
Software check integrity failures
Network attacks

Other auditable events are documented manually, such as CP/CPS violations, server room entry logs, and the like.

5.4.2 Frequency of Processing Log

No stipulation.

5.4.3 Retention Period for Audit Log

Audit logs are kept for a period of at least one year.

5.4.4 Protection of Audit Log

Access to logs is strictly limited to qualified system administrators and developers with credentials issued according to IT department control protocols. Audit logs may not be modified, and are protected from destruction throughout the retention period for those logs.

5.4.5 Audit Log Backup Procedures

No stipulation.

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Info Tech performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. Info Tech routinely assesses the systems and controls in place to protect the integrity of the Info Tech PKI system.

5.5 Records Archival

Info Tech complies with all record retention policies that apply by law.

5.5.1 Types of Records Archived

Info Tech retains the following information related to the operation of the Info Tech PKI system for archival purposes:

- Independent security assessment reports
- CP/CPS versions
- Contracts and other agreements concerning the operation of the Info Tech PKI system
- System and equipment configurations, modifications, and updates
- Identity authentication logs documenting the identification requirements of 3.2 *supra,* including information about telephone calls made for verification purposes and form of ID reviewed, for each subscriber
- Subscriber agreement versions
- CRLs
- Data necessary to verify an archive's contents
- compliance auditor reports
- Changes to audit parameters
- Attempts to delete or modify audit logs
- Certificate status changes and requests
- Appointments or removals of appointments of an individual to a trusted role
- Certificate compromise notifications
- Remedial actions taken as a result of violations of physical security
- Violations of the Info Tech CP/CPS

5.5.2 Retention Period for Archive

Archived records are retained for the life of the Info Tech PKI.

5.5.3 Protection of Archive

No stipulation.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

No stipulation.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Info Tech maintains incident response procedures to guide key personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. Info Tech reviews and updates its incident response plans as needed, but at least on an annual basis.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

Info Tech systems are protected by regular backups and Info Tech maintains copies of the Info Tech PKI system's private keys, which are stored securely. If Info Tech discovers that any of its systems have been compromised or corrupted, Info Tech assesses the danger, legal obligations, and possible risks associated with the incident. If Info Tech determines that a continued operation could pose a significant risk to relying parties or subscribers, Info Tech will suspend Info Tech PKI operations until the risk is mitigated, or as permitted by law.

5.7.3 Entity Private Key Compromise Procedures

No stipulation.

5.7.4 Business Continuity Capabilities after a Disaster

No stipulation.

5.8 CA or RA Termination

No stipulation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Keys will be generated on secure computers that have never been connected to any network. Those computers will be prepared using new storage media as provided by manufacturers, with software installed from read-only media such as DVD-ROM. The installation media will be stored for future examination, if ever needed, for as long as the certificates created with the keys are active.

Keys will be generated by trusted personnel using appropriate software, while observed by other trusted personnel who will document the procedure. The generated keys will be copied to previously unused external media, such as USB storage devices. After the keys have been generated, all persistent storage media used by the secure computers for this operation will be securely wiped and then physically destroyed.

The generated private keys will be kept in sealed containers in secure physical storage. When needed, the private keys will be removed and used by trusted personnel with trusted observers. There are two ways the private keys will be needed:

1. The root certificate private key will be used to sign new intermediate certificates as needed.
2. Intermediate certificate private keys will be installed into secure systems that will use them to sign end-user certificates upon proper controls and authorization.

All operations involving the root certificate keys will take place on secure computers as described above.

Intermediate certificate private keys will be encrypted using secure computers as described above, and then placed into service with systems that will decrypt and use them as authorized. Every time a private key is decrypted or used will be automatically logged.

6.1.2 Private Key Delivery to Subscriber

Private keys are generated by the Subscriber on their own computing equipment, and never leave their control. Subscribers may choose to back up their keys or to copy them to other computers under their control. In those cases, the private keys are strongly encrypted before being backed up or copied.

6.1.3 Public Key Delivery to Certificate Issuer

After the Subscriber generates a key pair, software on the Subscriber's own computing equipment is used to generate a Certificate Signing Request (CSR), which contains the public key and is digitally signed with the private key. The CSR is delivered to the Certificate Issuer over a secure Internet connection, where it is held until the Subscriber's identity has been confirmed, at which point the CSR is used to issue a Certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The CA Public Keys are contained in root and intermediate certificates that are available for download via a secure connection over the Internet.

6.1.5 Key Sizes

Subscriber's key pairs are 2048 bit RSA keys. The CA root and intermediate key pairs are 4096 bit RSA keys.

6.1.6 Public Key Parameters Generation and Quality Checking

RSA key pairs are generated with a 2048 bit modulus and a public exponent of 65537, using standard cryptographic software. Currently used software includes OpenSSL for CA key generation, and the Web Cryptography API for Subscriber key generation.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

Digital Signature, Non Repudiation, Key Encipherment

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CA private keys are stored either on physically locked external backup media, or encrypted using Amazon Web Services Key Management Service, with every decryption operation automatically logged for review.

Subscriber private keys are stored on their own computer's internal storage, encrypted using AES-256 with randomly generated keys stored on external servers and provided only upon Subscriber authentication.

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

No stipulation.

6.2.3 Private Key Backup

No stipulation.

6.2.4 Private Key Archival

No stipulation.

6.2.5 Private Key Transfer into or from a Cryptographic Module

No stipulation.

6.2.6 Private Key Storage on Cryptographic Module

No stipulation.

6.2.7 Method of Activating Private Key

No stipulation.

6.2.8 Method of Deactivating Private Key

No stipulation.

6.2.9 Method of Destroying Private Key

No stipulation.

6.2.10 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

No stipulation.

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Subscriber certificates are operational until revocation or expiration. Subscriber certificates expire 375 days after issuance.

CA intermediate certificates expire 10 years after creation. CA root certificates expire 40 years after creation.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No stipulation.

6.4.2 Activation Data Protection

No stipulation.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

Any computer system that creates or uses the root private key must be a freshly installed computer in which all writable media has been freshly removed from the manufacturer's sealed packaging, which is never connected to any network. All writable media is then either physically destroyed or placed in physically sealed, locked storage.

Any computer system that uses any intermediate certificate private key in unencrypted form must be secured from all user access (including administrator access), with all software installation and key decryption operations logged.

6.6 Life Cycle Technical Controls

No stipulation.

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

No stipulation.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

Systems with access to the root private keys must never be connected to any network.

Systems with access to intermediate private keys are network connected, but the private keys must always be encrypted with keys not on those systems, and only decrypted on systems that prevent all user or network access to the private keys. All decryption operations must be automatically logged.

6.8 Time-Stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

No stipulation.

7.1.1 Version Number(s)

No stipulation.

7.1.2 Certificate Extensions

No stipulation.

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

No stipulation.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

No stipulation.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

N/A

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

No stipulation.

8.2 Identity/Qualifications of Assessor

No stipulation.

8.3 Assessor's Relationship to Assessed Entity

No stipulation.

8.4 Topics Covered by Assessment

No stipulation.

8.5 Actions Taken as a Result of Deficiency

If an audit reports a material noncompliance with applicable law, this CP/CPS, or any other contractual obligations related to Info Tech's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify Info Tech, and (3) Info Tech will develop a plan to cure the noncompliance. Info Tech will submit the plan to the Executive Team for approval and to any third party that Info Tech is legally obligated to satisfy. The Executive Team may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected certificates.

8.6 Communication of Results

The results of each audit are reported to the Executive Team and to any third parties which are entitled by law, regulation, or agreement to receive a copy of the audit results.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Any fee associated with the issuance or renewal of a certificate is governed by other agreements which may or may not incorporate this CA/CPS.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Info Tech maintains Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2 Insurance or Warranty Coverage for End-Entities

Insurance coverage for end entities, if any, is specified in the Info Tech Relying Parties Agreement or another express agreement to provide insurance or warranty coverage to that entity.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information is considered confidential and, unless disclosed voluntarily, is protected against disclosure to the fullest extent permitted by law, regulation, or agreement:

- Business continuity, incident response, contingency, and disaster recovery plans;
- Non-public details of other security practices used to protect the confidentiality, integrity, or availability of information;
- Information held by Info Tech as private information in accordance with 9.4 *infra*;
- Audit logs and archive records; and
- Transaction records, financial audit records, and external or internal audit trail records and any audit reports.

9.3.2 Information Not Within the Scope of Confidential Information

Published information, including published and revoked certificate information, is not considered to be confidential information.

9.3.3 Responsibility to Protect Confidential Information

Info Tech's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive annual training on Info Tech procedures regarding the handling and protection of confidential information.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Info Tech maintains a comprehensive set of policies and procedures to safeguard personal information, client data, and other information. A summary of these practices and policies may be found in the Info Tech, Inc. Privacy Statement and Policy located at: https://www.infotechfl.com/legal/privacy_policy**.** More detailed information about Info Tech's Information Security Plan is available on request; for more information contact legal@infotechfl.com and request a current version of the Info Tech, Inc. Information Security Plan.

9.4.2 Information Treated as Private

Info Tech treats all identifying information about an individual that is not publicly available in the contents of a certificate or CRL as private, protected personal information according to the terms of our Info Tech, Inc. Privacy Statement and Policy located at: https://www.infotechfl.com/legal/privacy_policy.

9.4.3 Information not Deemed Private

Private information does not include certificates, CRLs, or their contents.

9.4.4 Responsibility to Protect Private Information

Info Tech employees and contractors are required to handle personal information in strict confidence and meet all applicable requirements for privacy protection and data security under applicable state laws or US laws. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5 Notice and Consent to use Private Information

Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a certificate. Info Tech will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All subscribers must consent to the global transfer and publication of any personal data contained in a certificate.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Info Tech may disclose private information, without notice, if Info Tech reasonably believes that the disclosure is required by law, regulation, or court order.

9.4.7 Other Information Disclosure Circumstances

See the Info Tech, Inc. Privacy Statement and Policy located at:
https://www.infotechfl.com/legal/privacy_policy

9.5 Intellectual Property Rights

Info Tech and/or its business partners own the intellectual property rights in Info Tech's services, including the certificates, trademarks used in providing the services, and this CP/CPS. "Info Tech" is a registered trademark of Info Tech, Inc. Certificate and revocation information are the property of Info Tech. Info Tech grants permission to reproduce and distribute certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. Info Tech does not allow derivative works of its certificates or products without prior written permission. Private and Public Keys remain the property of the Subscribers who rightfully hold them. All distributed elements of the Info Tech Private Keys are the property of Info Tech.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Except as expressly stated in this CP/CPS or in a separate agreement with a Subscriber, Info Tech does not make any representations regarding its products or services. Info Tech represents, to the extent specified in this CP/CPS, that:

- Info Tech complies, in all material aspects, with this CP/CPS, and all applicable laws and regulations,
- Info Tech publishes and updates CRLs and OCSP responses on a regular basis,
- All certificates issued under this CP/CPS will be verified in accordance with this CP/CPS and meet the minimum requirements found herein,
- Info Tech will maintain a repository of public information on its website, and
- Information published on a qualified certificate meets the requirements specified in US law.

To the extent allowed under US law, Info Tech:

- Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information,
- Is not responsible for information contained in a certificate except as stated in this CP/CPS,
- Does not warrant the quality, function, or performance of any software or hardware device, and
- Is not responsible for failing to comply with this CP/CPS because of circumstances outside of Info Tech's control.

9.6.2 Subscriber Representations and Warranties

Prior to being issued and receiving a Certificate, subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify Info Tech if a change occurs that could affect the status of the certificate. Subscribers represent to Info Tech and Relying Parties that, for each certificate, the Subscriber will:

- Securely generate its Private Keys and protect its Private Keys from compromise,
- Provide accurate and complete information when communicating with Info Tech,
- Confirm the accuracy of the certificate data prior to using the certificate,
- Promptly cease using a certificate and notify Info Tech if (i) any information that was submitted to Info Tech or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate,
- Use the certificate only for authorized and legal purposes, consistent with the certificate purpose, this CP/CPS, and the relevant Subscriber Agreement, and
- Promptly cease using the certificate and related Private Key after the certificate's expiration.

9.6.3 Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a Info Tech certificate, it:

- Obtained sufficient knowledge on the use of digital certificates and PKI,
- Studied the applicable limitations on the usage of certificates and agrees to Info Tech's limitations on liability related to the use of certificates,
- Has read, understands, and agrees to the Info Tech Relying Party Agreement (if applicable) and this CP/CPS,
- Verified both the Info Tech certificate and the certificates in the certificate chain using the relevant CRL or OCSP,
- Will not use a Info Tech certificate if the certificate has expired or been revoked, and
- Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a Info Tech certificate after considering:

  a) applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;

  b) the intended use of the certificate as listed in the certificate or this CP/CPS,

  c) the data listed in the certificate,

  d) the economic value of the transaction or communication,

e) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,

f) the Relying Party's previous course of dealing with the Subscriber,

g) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and

h) any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

- Any unauthorized reliance on a certificate is at a party's own risk.

9.7 Disclaimers of Warranties

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, INFO TECH DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. INFO TECH DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. Info Tech does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

9.8 Limitations of Liability

NOTHING HEREIN LIMITS LIABILITY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM INFO TECH'S NEGLIGENCE OR (II) FRAUD COMMITTED BY INFO TECH. EXCEPT AS STATED ABOVE, ANY ENTITY USING AN INFO TECH CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF INFO TECH RELATED TO SUCH USE, PROVIDED THAT INFO TECH HAS MATERIALLY COMPLIED WITH THIS CP/CPS IN PROVIDING THE CERTIFICATE OR SERVICE. INFO TECH'S LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS CP/CPS IS LIMITED AS FOLLOWS:

All liability is limited to actual and legally provable damages. Info Tech is not liable for: (1) Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if Info Tech is aware of the possibility of such damages; (2) Liability related to fraud or willful misconduct of the Applicant; (3) Liability related to use of a certificate that exceeds the limitations on use, value, or transactions as stated either in the certificate or this CP/CPS; (4) Liability related to the security, usability, or integrity of products not supplied by Info Tech, including the Subscriber's and Relying Party's hardware; or (5) Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether Info Tech failed to follow any provision of this CP/CPS, or (v) whether any provision of this CP/CPS was proven ineffective. The disclaimers and limitations on liabilities in this CP/CPS are fundamental terms to the use of Info Tech's certificates and services.

9.8.1 Indemnification by Info Tech

Info Tech shall does not agree to any indemnification obligations unless expressly stated in another agreement with the party to be indemnified.

9.8.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify Info Tech, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CP/CPS, or applicable law; (iii) the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of the certificate or Private Key.

9.8.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify Info Tech, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, this CP/CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.9 Term and Termination

9.9.1 Term

This CP/CPS and any amendments to the CP/CPS are effective when published to Info Tech's online repository and remain in effect until replaced with a newer version.

9.9.2 Termination

This CP/CPS and any amendments remain in effect until replaced by a newer version.

9.9.3 Effect of Termination and Survival

Info Tech will communicate the conditions and effect of this CP/CPS's termination via the Info Tech Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the certificate is revoked or expired, even if this CP/CPS terminates.

9.10 Individual Notices and Communications with Participants

Info Tech accepts notices related to this CP/CPS at the locations specified in Section 2.2 *supra*. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from Info Tech. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. Info Tech may allow other forms of notice in its Subscriber Agreements.

9.11 Amendments

9.11.1 Procedure for Amendment

This CP/CPS is reviewed from time to time, but at least annually. Amendments are made by posting an updated version of the CP/CPS to the online repository. Controls are in place to reasonably ensure that this CP/CPS is not amended and published without the prior authorization of Info Tech

9.11.2 Notification Mechanism and Period

Info Tech posts CP/CPS revisions to its website. Info Tech does not guarantee or set a notice-and-comment period and may make changes to this CP/CPS without notice and without changing the version number. Major changes affecting accredited certificates are announced and approved by the accrediting agency prior to becoming effective. Info Tech is responsible for determining what constitutes a material change of the CP/CPS

9.11.3 Circumstances Under Which OID Must be Changed

Info Tech is solely responsible for determining whether an amendment to the CP/CPS requires an OID change.

9.12 Dispute Resolution Provisions

Parties are required to notify Info Tech and attempt to resolve disputes directly with Info Tech before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution

9.13 Governing Law

This CP/CPS is governed by the laws of the State of Florida without regard to the state's conflict of laws provisions. Any action brought against Info Tech arising from the operation of the policies and procedures described in this CP/CPS can only be brought in the applicable state or federal courts located in Alachua County, Florida.

9.14 Compliance with Applicable Law

This CP/CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptographic products. Subject to section 9.4.5’s Notice and Consent to Use Private Information contained in Certificates, Info Tech has established appropriate technical and organizational measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.15 Miscellaneous Provisions

9.15.1 Entire Agreement

In the absence of another express agreement with Info Tech, this CP/CPS states the entirety of the rights and obligations of Info Tech and any entity that may have rights or obligations arising from the operation of the policies and procedures described in this CP/CPS.

9.15.2 Assignment

No entity with rights or obligations arising from the operation of the policies in this CP/CPS may assign those rights or obligations without the prior written approval of Info Tech.

9.15.3 Severability

If any provision of this CP/CPS is adjudicated by a court or other tribunal of competent jurisdiction to be unenforceable, the remainder of this CP/CPS will remain valid and enforceable,

9.15.4 Enforcement (Attorneys' Fees and Waiver of Rights)

Info Tech may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. Info Tech’s failure to enforce a provision of this CP/CPS does not waive Info Tech’s right to enforce the same provision later or right to enforce any other provision of this CP/CPS. To be effective, waivers must be in writing and signed by Info Tech.

9.15.5 Force Majeure

Info Tech is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond Info Tech’s reasonable control. The operation of the Internet is beyond Info Tech’s reasonable control.