



The Federation for Identity and
Cross-Credentialing Systems®

FiXS[®] Policy Document
Version 3.0
September 1, 2010

www.fixs.org

Copyright 2010 by the Federation for Identity and Cross-Credentialing Systems®, Inc.

All Rights Reserved

Printed in the United States of America

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

TABLE OF CONTENTS

1.0	GENERAL REQUIREMENTS AND DEFINITIONS.....	3
2.0	EXECUTIVE OVERVIEW	3
3.0	U.S. FEDERAL AGENCIES AND U.S. DEPARTMENT OF DEFENSE INTERFACES	6
4.0	FIXS MEMBER, SUBSCRIBER, AND CREDENTIAL HOLDER REQUIREMENTS.....	6
5.0	SECURITY	7
6.0	PRIVACY POLICY AND STATEMENT	8
7.0	INTELLECTUAL PROPERTY POLICY STATEMENT	12
8.0	ANTI-TRUST POLICY STATEMENT.....	15
9.0	CONFLICT OF INTEREST POLICY	21
10.0	TERMS OF USE OF FIXS INTELLECTUAL PROPERTY AND LICENSING	25
11.0	BRAND, TRADEMARK, AND GRAPHICS POLICY.....	28
12.0	DISASTER RECOVERY	35

1.0 GENERAL REQUIREMENTS AND DEFINITIONS

The purpose of this policy document is to set forth the policy framework and principles of operations of the Federation for Identity and Cross-Credentialing Systems, Inc®.(FiXs®). This policy framework is integral with other FiXs foundational and governance documents, rules, and procedures, which include, but are not limited to the: FiXs Bylaws, FiXs Operating Rules, FiXs Implementation Guidelines, FiXs Trust Model, FiXs Security Guidelines, FiXs Technical Architecture Specifications as well as the processes, the physical systems and architecture and all other elements and components of the FiXs Network.

2.0 EXECUTIVE OVERVIEW

Introduction

The Federation for Identity and Cross-Credentialing Systems (FiXs) is comprised of private companies of various sizes, not-for-profit organizations, and government organizations that support and contribute ideas, knowledge, and technologies associated with implementing a secure identity cross-credentialing network that is based on open standards, world-class processes, and proven, industrial-strength technologies and security. Similar to the financial industry in managing transactions across a myriad of financial organizations securely and reliably through their trusted financial networks, FiXs has developed an interoperable electronic means of authenticating individuals who are duly vetted through a series of audited procedures and certifying authorities to ensure system integrity.

The Federation provides a federated identity management network and certified system solutions and capabilities to provide member organizations the ability to authenticate individuals' identities. The network supports member organizations in: business to business; government to business; and business to government transactions from other member organizations which may be different, or unknown, to that organization. This capability is provided with a high-degree of accuracy and "trust" through the application of a Federated Trust Model enforced by FiXs. These solutions and capabilities can be utilized worldwide, in remote or fixed environments, wired or wirelessly, and in real-time. The network also supports revocation processes within a three-hour span.

To be clear, FiXs itself is predominantly a standard – setting body with a Governance Model, to include Trust Model. FiXs itself does not deploy nor implement identity authentication technologies or capabilities. Other than managing the oversight of the FiXs Trust Broker (through the Configuration Control Board and Executive Committee), all FiXs-based components and

capabilities are implemented by commercial entity FiXs members who have met certain deployment standards and been certified and/or authorized by FiXs to operate.

History

FiXs was formed as a coalition, in 2002, in piloting a federated identity transaction model and was incorporated as a 501(c) 6 not-for-profit corporation in 2004. FiXs maintains its' status as a 501(c) 6 "trade association" consistent with the requirements of the U.S. Internal Revenue Service and a corporation standing under the laws of the Commonwealth of Virginia. A long-standing affiliation with the Defense Manpower Data Center (DMDC) and its Defense Cross-Credentialing Identification System (DCCIS) program has enabled participating Department of Defense and industry members to achieve secure and interoperable identity verification and authentication for secure facility access. In 2005, FiXs was selected as the FCW Events Government Solution Center Pioneer Award for most "Successful Public/Private Sector Partnership." The award singled out FiXs for recognition as a premier example of a program managed collaboratively by government and non-government partners that tangibly improved government operations and that of their commercial counterparts.

Operations

The FiXs Network and FiXs-certified solutions employ a Federated Trust Model, allowing the broadest range of disparate organizations to inter-operate and authenticate identities and then to locally manage privileges. The essential underpinnings of the FiXs Federated Trust Model are based on two inter-related parts: a trusted organization and a trusted individual identity within that organization. The two parts are linked through a "chain of trust" process that permits vetted and trusted organizations the ability to create and issue an individual's identity credential that can be authenticated and managed over the trusted and secure network by other members of the Federated Trust Model. Once the identity credential is established in this manner, it can be used in various role-based workplace environments to assign privileges consistent with the objectives and unique requirements of that member organization. FiXs' role is limited to identity authentication, which occurs prior to role, privilege designations, or authorizations being assigned by member organizations. This identity authentication model can support either physical or logical privilege or "authorization" designations.

The FiXs Network applies currently proven and available identity management technologies, in conjunction with biometric identification and can be used to verify the identity of personnel seeking to physically enter government or military-controlled areas, as well as the widest range of commercial facilities as well

logical access to their systems or applications. FiXs can be used within and between public and private sector organizations and promotes a trusted mechanism for federated identity infrastructures. The FiXs interoperable identity authentication network also is currently the only network certified to inter-operate with the Defense Cross-Credentialing System (DCCIS) of the United States Department of Defense.

FiXs does not grant or deny physical or logical access or determine authorization privileges. Rather, it delivers a trusted **infrastructure and authentication service** that provides participating members with the necessary high confidence in the actual identity of individuals requesting access to facilities and systems. The results of the FiXs Network authentication requests can be used by facility and system managers to determine independently whether they will grant or deny access or other privileges based upon their own unique business process needs.

Privacy and Trust

FiXs is unique in that it does not replicate or store identity factors in a single data store. All personal identity information of individuals is kept and maintained at the location of or designated by the organizational sponsor of the individual in a federated manner. As such, personal identity information is “written and stored” once, at the “home location” of the individual. That information is then validated across the network with the applicable “home location” of the individual at the time a credential is presented for authentication.

PIV-1 Aligned and PIV-Interoperable (“PIV-I”)

FiXs employs a set of Operating Rules consistent with Part 1 (PIV-1) of standards issued to implement Homeland Security Presidential Directive 12 (HSPD-12). The Directive seeks to create a “mandatory, government-wide standard for secure and reliable forms of identification issued by the U. S. Federal Government to its employees and contractors (including contractor employees).” Designed to meet these requirements, FiXs provides a secure and certified network that can handle identity transactions consistent with Federal Information Processing Standard (FIPS) 201, Personal Identity Verification Part 1 (PIV-1). Only Federal government organizations can issue PIV credentials, but each Federal entity can choose to accept PIV “aligned” (PIV – 1) or PIV – Interoperable (“PIV – I”) credentials following accepted certification and assessment criteria by the Federal entity. The Department of Defense (DoD) is accepting PIV “aligned” credentials via the FiXs Network through the DoD’s DCCIS infrastructure.

3.0 U.S. FEDERAL AGENCIES AND U.S. DEPARTMENT OF DEFENSE INTERFACES

In its' initial phase, FiXs successfully worked with the U. S. Department of Defense (DoD) in establishing a mutually-trusted, inter-operable community wherein DoD contractors, vendors and trading partners are able to exchange approved data to authoritatively authenticate their identities. Currently, FiXs is the only organization inter-operable with DCCIS.

FiXs and the Department of Defense's Defense Manpower Data Center (DMDC) have signed a formal Memorandum of Understanding attesting to maintaining this trusted relationship with the DoD. FiXs is committed to including other partners throughout the Federal Government, such as the first responder community, and with other public and private sector organizations, both in the United States and internationally that seek a secure, scalable, rules-based, inter-operable identity authentication capability.

- 3.1 Federal Agencies or the DoD, as applicable, have the responsibility for informing Federal/DoD facilities and locations participating in the FiXs Network of the FiXs policy and procedures, as they may apply to them. The DoD also operates and maintains the Department of Defense's Trust Gateway Broker ("DCCIS router") and administers the Defense Cross-Credentialing Identification System (DCCIS) Rules allowing identity cross-authentication with the FiXs Network.
- 3.2 DoD members that have been issued a DoD Common Access Card (CAC) fulfill the current criteria as set by the FiXs Trust Model and, as they are registered in DCCIS, they will be allowed to have their credential authentication attributes pass across the FiXs Network.
- 3.3 This policy does not prescribe that Federal Agencies or DoD facilities and/or installations recognize FiXs members enrolled in the FiXs Network physical or logical access privileges. Access to any Federal/DoD facility or system is subject to the sole determination of the Federal/DoD site Security/Access Control Official for that federal facility or system, as applicable.

4.0 FiXs MEMBER, SUBSCRIBER, AND CREDENTIAL HOLDER REQUIREMENTS

FiXs, all FiXs Members in any membership category, subscribers, individual credential holders and all entities or individuals participating in the operations of the FiXs Network or who possess FiXs-certified Credentials have an affirmative responsibility to uphold and support the governance and operational rules and

policies of the Federation. Any misuse, abuse, or negligence in supporting these affirmative obligations may result in having such entities or individuals' ability to participate in any such capacity within FiXs or on the FiXs Network revoked along with being subject to any other criminal or civil penalties that may be available. Each FiXs participating industry member is responsible for ensuring that all industry facilities and locations participating in the FiXs Network will fully implement the FiXs policies and Trust Model and the procedures as defined in the FiXs Operating Rules.

5.0 SECURITY

The intent of this section is to ensure the integrity and availability of all FiXs connected systems, and to ensure the security and privacy of the data stored, generated, and processed by the FiXs Network. Further, it is the intent of this policy in any of its manifestations to ensure secure inter-operability with relevant DoD Networks. Additional guidelines, procedures, and technical implementations are detailed in the FiXs Security Guidelines.

- 5.1 All individuals and organizations subject to this policy shall use reasonable and practicable measures to ensure that:
 - Information will be protected from unauthorized access.
 - Confidentiality of information is assured.
 - Integrity of information is maintained.
 - Regulatory and legislative requirements are met.
 - Systems are maximally available to perform their defined functions.
 - Access to data is restricted only to those who have a specific need and authorized access.
 - All changes are logged.
 - Privacy of individual's data is appropriately protected.
- 5.2 All individuals and organizations subject to this policy shall be responsible for implementing and monitoring such security technologies and procedures as required to address the objectives of this policy.
- 5.3 All individuals and organizations subject to this policy shall be responsible for reporting any breach of this policy and for remediation, as appropriate.
- 5.4 Compliance with this security policy is subject to audit by FiXs as well as certain government authorities. Documented failure to comply with this security policy is grounds for denial of access to the FiXs Network and revocation of credentials.

6.0 PRIVACY POLICY AND STATEMENT

The Federation for Identity and Cross-Credentialing Systems, Inc. (“FiXs”) recognizes that the individuals who participate in the FiXs Network value their privacy. Protecting individual privacy is also important to FiXs. To provide notice and information to users and suppliers to the FiXs Network, FiXs is furnishing this Privacy Policy and Statement setting forth FiXs’ privacy policy related to creating and managing credentials and authentication inquiries on the FiXs Network or FiXs-certified Credentials. Use of the FiXs Network is governed by the following documents:

FiXs Trust Model*
FiXs Policy Statements/Guidelines*
FiXs Operating Rules*
FiXs Security Guidelines*
FiXs Technical Architecture and Specifications*
Federal Privacy Act

* As amended from time-to-time by FiXs

The Trust Model imposes obligations on all organizations participating in the FiXs Network to secure and protect all personally identifiable information (“*personal information*” or “*PII data*”) in conformance with the minimum standards outlined in the documents listed above. This Privacy Policy and Statement (“**Privacy Statement**”) describes the minimum privacy practices to be applied by all FiXs-certified Credential issuers and FiXs Network service provider(s) in connection with the governance model, to include the FiXs Trust Model and FiXs Operating Rules.

All FiXs member companies are expected to implement personal information protection policies to the extent practicable, and in compliance with respective laws. This includes providing notice to individuals about what the member company will do with their personal information; choice for the individual with regard to the provision of any discretionary personal information; access for the individual to information held by the member company, including the opportunity to correct personal information and a redress process if decisions are made in light of inaccurate personal information; security procedures for the systems holding personal information; and a proper enforcement process for company employees who violate those privacy policies.

The following policy serves as the standards for the collection, use, retention, and security of personal information for **all** persons or organizations that provide services in connection with the FiXs Network.

Collecting Personal Information

In order to accomplish the objective of authenticating personal identity among and between relying parties (“**Relying Parties**”) subscribed to the FiXs Network, the following personal information is collected and stored by the issuer as described below:

- a. Individual first name, last name and middle initial
- b. Employee identification number
- c. Digital photograph
- d. 10 fingerprints, as applicable
- d. A copy of the completed Immigration and Naturalization Service Form I-9.
- e. Two government-issued picture identification documents i.e. “breeder documents”
- f. Other identifying personal information that is necessary for the “trust level” of credential that the individual is applying for, as prescribed by the entity who sponsors the individual as a user

The entity that sponsors individual users is referred to as the “**Subscribing Party**.” The Subscribing Party will select a FiXs-certified solution provider to enroll, issue credentials, and manage the users that the Subscribing Party sponsors to receive a FiXs-certified Credential. The sponsor will designate the single secure Provider location that will serve as a central repository of its’ sponsored users’ personal information for purposes of identity authentication using the FiXs Network. Personal information may only be stored at this single location and may not be replicated or passed across the FiXs Network. This information will be retained for the longest period required by applicable laws or regulations.

Any personal information that is obtained solely for the purposes of vetting ones’ identity for credential issuance purposes is not required to be maintained or stored for FiXs Network authentication purposes. However, an employer or sponsor may store such information for its own records retention purposes in accordance with its own regulatory, statutory, or business requirements. In such cases, that employer or sponsor should inform the credential holder as to its record retention policies, procedures, and practices.

Disclosures of Information

Neither FiXs nor its certified Credential Issuers or solution providers shall disclose or otherwise transfer any personal information collected for credential issuance purposes, except as specified in this policy. FiXs-certified Credential Issuers and service providers are each responsible to ensure the compliance of their contractors and agents with this Privacy Statement. Certain personal information provided for credential authentication purposes will be accessible to

parties relying upon the FiXs-certified Credential that may be presented for authentication purposes.

Consistent with applicable laws and regulations, information collected about individuals who possess FiXs-certified Credentials for authentication purposes may be shared as necessary for authorized law enforcement, homeland security, or national security activities.

Use of Personal Information in Cross-Credentialing for the Purpose of Identity Authentication

Except as specified in this Privacy Statement, the personal information an individual provides for identity authentication shall not be used by any party for any other purpose.

When seeking entry to selected facilities, application, or systems of organizations, agencies, companies, or Relying Parties that are participating in the FiXs Network, an individual may be asked to produce information or provide personal information, including one or more fingerprints. This information will be transmitted across the FiXs Network, in an encrypted form, and compared with information held by the FiXs-certified Solution Provider designated by the individual's sponsor to retain such person's personal information. The FiXs-certified Solution Provider will perform a comparison of the data on file and will transmit the results of this comparison, in an encrypted form, to the Relying Party making the authentication request. Personal information that is sent for authentication to the Relying Party facility or system that an individual seek to access will not be retained by that Relying Party, but such party may create its own record of such individual's credential authentication and request for access.

All decisions regarding access, or privileges to be granted, to participating facilities and systems will be controlled by the operators of such facilities or systems based on the criteria they have independently established.

The FiXs-certified Solution Provider will keep logs of identity authentication requests received from participating parties. These logs will be retained for the purpose of audit, compliance, and other authorized purposes.

Security Procedures

The FiXs Network maintains physical, electronic, and procedural safeguards that comply with U.S. government standards to protect an individual's personal information. These safeguards are routinely monitored and communicated to FiXs representatives and FiXs Network Solutions Providers, Credential Issuers and sponsoring or subscribing parties. Each Network Solutions Provider, Credential Issuer, and sponsoring party is responsible to protect personal

information from unauthorized disclosure or loss, at a minimum, in accordance with such safeguards. Without limiting the foregoing, an individual's personal information will be stored in a database secured in at least the same manner that the individual's sponsor generally protects the personal information of its employees.

For security purposes and to ensure that the credential authentication service remains available to all users, FiXs employ software programs to monitor traffic to identify unauthorized attempts to access, upload, or change information, or otherwise cause damage.

Any Network Solutions Provider, Credential Issuer or sponsoring party that becomes aware that personal information has been disclosed or used other than in accordance with this Privacy Statement, including any unauthorized disclosure or loss of information, should immediately notify FiXs in writing of such event, and cooperate fully with FiXs in investigating the relevant circumstances. An individual that becomes aware that personal information has been disclosed or used other than in accordance with this Privacy Statement, including any unauthorized disclosure or loss of information, should immediately notify the applicable sponsor and FiXs in writing of such event, and cooperate fully with such sponsor and FiXs in investigating the relevant circumstances.

Any FiXs Solution Provider, Credential Issuer, or Subscribing Party that breaches its obligations under this Privacy Statement with respect to personal information will defend, indemnify, and hold harmless FiXs, and its officers, directors, employees, contractors and agents, from and against all liabilities, damages, expenses (including reasonable attorneys fees and costs), fines, and claims of any kind or based on any legal theory, arising from or relating to such breach.

Notification of Changes

FiXs reserves the right to change, modify, or update this Privacy Statement at any time without notice. The current version of all such governance documents will be maintained on the FiXs website (www.fixs.org). All interested persons and entities should review the published Privacy Statement regularly in order to remain knowledgeable about the Privacy Statement and any revisions to it.

How to Contact Us

FiXs' Privacy Statement is available on the FiXs web site at www.fixs.org. Any questions concerning the FiXs privacy policies should be directed to the FiXs Administrator by telephone at 703-591-9255.

7.0 INTELLECTUAL PROPERTY POLICY STATEMENT

Purpose

The purpose of this FiXs Intellectual Property Policy Statement (“**IP Policy**”) is to set forth FiXs’ policy as it pertains to the creation, management, and ownership of the intellectual property developed through the activities of FiXs or otherwise owned or licensed by FiXs.

Applicability

This IP Policy applies to all FiXs member firms in all membership categories and all FiXs officers, directors, employees, contractors and contract employees, including all individuals who support the various FiXs committees and work groups or participate in other FiXs meetings, past, present and future. This policy covers all types of intellectual property, including patents, copyrights, trade secret and other proprietary rights of any kind, e.g., inventions; discoveries; trade secrets, trademarks, service marks, writings, art works, software, and other literary works.

Background

FiXs is a registered tax-exempt, 501(c) 6 trade association whose objectives are to establish standards and, provide objective oversight of the FiXs Network and to provide a forum for discussing, defining, and developing necessary operating rules, policies, guidelines and implementation standards for use by Network users. These activities entail providing an open and trusted environment where interoperable procedures, processes, and technologies can be tested and implemented. The goal of those activities is to allow FiXs’ commercial users and the government; including the Department of Defense and U.S. civilian agencies, state and local governments and agencies (including first responders and emergency personnel), along with their contractors and constituents, to interact in a secure, efficient, and effective manner without being unduly subject to proprietary technologies or vendor influence, or having to create redundant, ineffective, or inefficient systems.

FiXs is an “open membership” organization comprised of systems integrators, solution providers, technology firms, financial institutions, consulting companies, not-for-profit associations, and various other organizations (including government agencies) representing a large community of interest, contributing in an open forum to pursue the deployment and use of open, inter-operable, and accessible industry standards, technologies, and processes to authenticate secure identity credentials.

License to Use

Expressly authorized members of FiXs may be licensed to use the intellectual property of FiXs in providing identity authentication solutions to their customers or other parties consistent with the terms of specific licensing agreements.

Proprietary Rights

Based upon the authority in the FiXs Bylaws and Operating Rules, FiXs may grant designated Members a non-exclusive license to possess and use all or portions of FiXs' Work Product(s) and Pre-existing Property, as identified in this Policy, that are required for a Member to make use of the FiXs Network consistent with the Operating Rules. FiXs may also grant authorized Members the right to grant to FiXs Issuers and FiXs Relying Parties a sublicense to possess and use those portions of the FiXs Work Product and Pre-existing Property required for a Member to make use of the FiXs Network solely in accordance with the Operating Rules.

Each Member will promptly identify to FiXs any specific portions of the Member's intellectual property that may need to be furnished to FiXs, other Members or other users to enable FiXs, its Members or other users to use or modify elements of the FiXs Network. To facilitate such purposes, the respective Member hereby grants to FiXs a non-exclusive, perpetual, worldwide, royalty-free, irrevocable license to copy, modify, distribute, display, perform, make, import and have made, and sublicense to its other Members, Credential Issuers, Issuer Sponsors, Network Service Providers, Member Service Providers, Members and other users of the FiXs Network, all intellectual property, including software, of that Member that is included in or integral to the operation of the FiXs Network or the FiXs Work Product, for purposes of the use, operation, support or enhancement of the FiXs Network. To the extent a Member wishes to obtain further clarification of such license grant, the Member and FiXs will work together to develop the appropriate form of license terms and conditions to govern any license or sublicense to be granted by any Member to the operators or users of the FiXs Network, provided that FiXs shall retain the sole authority to approve the final form and content of such license terms and conditions. Each Member's intellectual property that (1) is not the FiXs Network or FiXs Work Product or a modification of the FiXs Network or FiXs Work Product, (2) adds functionality to the FiXs Network or FiXs Work Product (i.e., the FiXs Network or FiXs Work Product are not dependent on it) and (3) was or is created without funding from FiXs, directly or indirectly, shall belong to such Member and shall not be subject to the above-stated license grant.

FiXs shall have sole and exclusive intellectual property ownership rights in any and all work product created or developed by all FiXs officer, directors, employees, contractors and contract employees, as well as any individuals who

support the various FiXs committees and work groups or participate in other FiXs meetings, regarding work product prepared by or for FiXs (“**FiXs Work Product**”).

Any intellectual property, including software that existed before such FiXs Work Product was created or that is created thereafter, other than for or on behalf of FiXs, shall remain the property of the respective owner, subject to the above-stated license grant to FiXs and its Members. In addition, intellectual property funded by or developed at FiXs expense shall be and remain the sole and exclusive property of FiXs.

FiXs Work Product and Pre-existing Property for FiXs Network

- FiXs brand, marketing collateral, FiXs-branded documents, trademark, and all other marks or designations of FiXs
- FiXs Bylaws
- FiXs Operating Rules/Guidelines
- FiXs Policies and Procedures
- FiXs Trust Model
- FiXs Security Guidelines
- FiXs Technical Architecture Specification
- FiXs Network (as defined in the FiXs Bylaws, Version 3.0, September 1, 2010, 2006, page 2, Article I, Section 4, paragraph a.), and associated interfaces
- FiXs Trust Gateway Broker (TGB) software, components and any additional TGBs to be established in the future
- FiXs software and software interfaces related to the FiXs domain server (FDS)
- FiXs software related to the authentication stations and various configurations thereto
- FiXs Recommendations for Creating a Unique Identifier for FIPS 201-aligned FiXs Credential (CHUID)
- FiXs Network additions, enhancements, updates, all associated software code versions, and all documentation related to the above artifacts.

* As may be revised, amended or modified from time to time. Other property may be created subsequent to this date, which will be similarly included.

Compliance

All member companies and individuals have an obligation to protect FiXs' intellectual property rights and an ongoing obligation not to infringe upon those rights. Strict compliance with this policy is also a condition of membership in FiXs.

It is the policy of FiXs vigorously to enforce the provisions of this IP Policy to the fullest extent of the law.

If there are questions about, or perceived violations of, this IP Policy, members will promptly report such matters to the FiXs President or FiXs Corporate Secretary.

8.0 ANTI-TRUST POLICY STATEMENT

Purpose

The Federation for Identity Cross-Credentialing Systems, Inc. ("FiXs"), a tax-exempt, 501(c) (6) trade association consisting of commercial and other non-profit entity members, as well as government agency participants, recognizes and endorses the policies underlying the nation's antitrust laws. Activities that intentionally or unintentionally reduce competition or restrain trade are contrary to FiXs' belief in competition and FiXs policy. In order to ensure that FiXs members, directors and staff understand and comply with the antitrust laws and FiXs policy, the FiXs Board of Directors has adopted the following Antitrust Policy Statement.

FiXs' activities consist of efforts by its commercial and non-profit members, as well as government agency participants, pertaining to the design, development or application of theoretically interchangeable identity management solution sets. One of FiXs' objectives is to establish a Network that will serve as a trusted environment in which interoperable identity management procedures, processes, and technologies can be tested and implemented. The goal of those activities is to allow FiXs' commercial users and government agencies such as the U.S. Department of Defense and civilian agencies, state and local governments and agencies (including first responders and emergency personnel), along with the agencies' contractors and constituents, to interact effectively and efficiently with respect to identity management.

These trade association activities are subject to federal and state antitrust laws. A trade association may be held legally responsible for the authorized and, under certain circumstances, unauthorized acts of its members that violate the antitrust laws. Therefore, in all FiXs activities, each member and FiXs staff is responsible for following FiXs' policy of compliance with all antitrust laws. FiXs officers, directors, committee chairs, and FiXs staff are responsible for making this policy known to all members of FiXs and for ensuring compliance in the course of activities pursued by FiXs.

Overview of the Antitrust Laws

FiXs and its members are subject to both federal and state antitrust laws. The federal antitrust laws are intended to prevent a wide range of conduct that interferes with or threatens to interfere with competition. In addition, most states have enacted antitrust laws that generally parallel the federal antitrust laws. The most important antitrust statutes relating to an association's activities are as follows:

Section 1 of the Sherman Act in broad terms prohibits "every contract, combination . . . or conspiracy" in restraint of trade. This prohibition covers all types of anticompetitive agreements or contracts, including but not limited to price-fixing agreements. The Sherman Act prohibits any agreement among current or potential competitors that affects any component of the price of a product or service, regardless of the purpose of the agreement and regardless of whether the price agreed to is "fair" or "reasonable." An agreement among buyers that fixes the price they will pay for a product or service is likewise prohibited. "Price" is defined broadly under the law to include all price-related terms, including discounts, rebates, commissions, and credit terms. Agreements among competitors to fix, restrict, or limit the amount of a product or service that is produced or offered may be treated the same as a price-fixing agreement.

Section 1 also prohibits, among other practices, bid-rigging agreements among actual or potential competitors, market or customer allocation agreements among competitors, and certain group boycott agreements.

An unlawful agreement need not be formal or reduced to writing; unlawful agreements may be inferred from circumstantial evidence, such as competitors taking parallel action on prices after discussing prices at a meeting, even if there were no express words of agreement at the meeting. An association's members and staff must also remember that the Sherman Act is a criminal conspiracy statute. If you are not an active participant - if you merely sit by at a meeting while the members of the association engage in an illegal discussion concerning price-fixing, you may be held criminally responsible, even though you said nothing during the discussion.

Section 5 of the Federal Trade Commission Act prohibits "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in

or affecting commerce.” This broadly worded statute prohibits conduct that would violate one of the other antitrust laws, such as price-fixing, as well as practices that closely resemble other antitrust violations in their adverse effect on competition. The Federal Trade Commission Act reaches anticompetitive acts committed by single persons or companies whether or not there is any agreement or “combination;” it also covers joint actions. The FTC has broad power to determine what constitutes an unfair method of competition or unfair or deceptive act or practice under any given circumstances.

Penalties for Violation of the Antitrust Laws

Violations of the antitrust laws can have very serious consequences for FiXs, its members, and their employees. The Sherman Act is a criminal statute. Violations of the act may be prosecuted as felonies and are punishable by steep fines and imprisonment for up to ten years. In addition, the federal government, state attorneys general, and any person or company claiming to have been injured by an antitrust violation may sue to recover three times the amount of the damages, plus attorney’s fees.

The maximum statutory antitrust fines are \$100 million for corporations and \$1 million for individuals. The size of an organization’s fine may be increased, however, to as much as twice the pecuniary gain derived from the offense or twice the loss suffered. This can be a very large number; antitrust fines for corporations exceeding \$10 million have become common and some fines have topped \$100 million. The collateral consequences of an antitrust conviction can be devastating for corporations. They include debarment from federal contracting, exposure to follow-on treble damages suits by private parties, which are often filed as class actions, exposure to investigations and enforcement actions in other countries, disruption of business, and the expense of defending antitrust investigations and lawsuits. In addition, the events surrounding an antitrust violation may provide the basis for other charges. Prosecutors often combine antitrust charges with allegations of wire fraud, mail fraud, and providing false statements to the government, all of which carry additional penalties.

For individuals, the consequences of involvement in an antitrust offense include, in addition to potential fines and jail time, loss of job and benefits, loss of reputation, loss of future employment opportunities, and exposure to litigation.

Violation of the Federal Trade Commission Act can result in issuance of a cease and desist order, which can place extensive governmental restraints on the activities of an association and its members or call for dissolution of the trade association itself. Failure to obey such an order can result in penalties of as much as \$10,000 per day.

Recognize and Avoid High-Risk Conduct

Certain antitrust violations are so likely to result in criminal prosecution that they are often referred to as “hard core” offenses. Conduct that falls in this category is

automatically illegal; absence of actual anticompetitive effects will not be a defense. Conspiracies among actual or potential competitors to restrict competition are in this category, and include the following:

Price-Fixing Agreements

the government strictly enforces the price-fixing prohibitions of the Sherman Act. A price-fixing violation may be inferred from similar price behavior by an association's members, even in the absence of a written or oral agreement.

Agreements to Allocate Customers or Markets

Agreements among competitors (or potential competitors) to allocate or divide markets, territories, customers, or sales channels are automatically illegal and are often prosecuted as criminal offenses. Even an informal agreement whereby one company agrees to stay out of another's territory or not to solicit its customers constitutes a violation of the antitrust laws.

Bid-Rigging Agreements

Agreements or understandings among competitors (or potential competitors) on any method by which prices or bids will be determined, quoted, or awarded are illegal. This includes: rotating bids; agreements regarding who will bid or not bid; agreements establishing who will submit bids to particular customers or for particular projects; and exchanging or advance signaling of the prices or other terms of bids. Bid rigging is nearly always prosecuted as a criminal offense.

Other Potentially Risky Conduct

There are other activities which, though typically not subject to criminal prosecution, are nevertheless potentially high-risk because they frequently lead to investigations or lawsuits, and a finding of liability may have severe adverse consequences.

Group Boycotts

An agreement with competitors, suppliers, or customers not to do business with another party, or to use concerted economic leverage against another party, may be found illegal as a boycott or "concerted refusal to deal."

Membership Restrictions

Assuming that the members of an association derive an economic benefit from membership, the denial of membership to an applicant may constitute a restraint of trade if it substantially impairs the ability of the applicant to compete and is not based on objective criteria. Similarly, no member of a trade association can be forced to participate in discussions or to attend association meetings.

Exclusionary Standardization and Certification And Self-Regulation

Association voluntary standardization and certification programs and self-regulatory programs such as industry codes of ethics generally are pro-competitive and lawful. Such activities may be found unlawful, however, if they have the effect of fixing prices or if they injure competition by unreasonably excluding some firms from a market, limiting output of products or services, or discouraging innovation. Standards and certification programs and industry self-regulatory programs should be conducted according to principles of voluntarism, objectivity, and due process. "Due process" means: all stakeholders have a right to participate in the formation of the standard, certification criteria, or code of ethics; the process is open and free from dominance by any particular industry segment or company; and there is a right to appeal from adverse decisions.

FiXs Anti-trust Policy and Guidelines

It is the policy of the FiXs that no member, director, or staff member shall:

- Seek or enter an agreement among competitors to fix or stabilize prices
- Seek or enter an agreement among competitors to limit production
- Hinder non-members' access to any market
- Economically coerce members
- Seek or enter an agreement not to do business with any party, or to do business with another party only on specified terms
- Seek or enter an agreement among competitors to allocate markets, territories, or customers
- Otherwise unreasonably restrict competition or engage in activity violative of any antitrust law.

In order to ensure that the above policy is fully implemented, the FiXs Board of Directors has adopted the following guidelines:

General Guidelines

1. A full description of the FiXs' intent to comply fully with the antitrust laws will be included in its written Policy Statement.
2. All FiXs members, directors, committees and staff shall receive and familiarize themselves with the FiXs' Antitrust Policy Statement.
3. FiXs' legal counsel will periodically update members, directors and staff concerning antitrust issues and review FiXs' antitrust compliance.
4. FiXs' legal counsel will approve in advance all new FiXs programs or changes in existing programs that may have potential antitrust implications.

5. If possible, all FiXs meetings, including conference calls, shall be regularly scheduled and all members should receive reasonable advance notice. In no case shall members hold informal “rump” meetings.
6. An agenda will be prepared for each FiXs meeting, and the agenda shall be reviewed in advance by legal counsel
7. Understand the purposes and authority of each FiXs committee or other group in which you participate.
8. If possible, legal counsel will be present at all meetings of the Board of Directors and at any other meeting at which sensitive issues will be discussed.
9. The minutes of all Board and Committee meetings, as applicable, will be reviewed by legal counsel before their approval and dissemination.
10. The minutes of all FiXs meetings will be accurate, and the association executive will not sign minutes that are materially inaccurate or incomplete.
11. Any action by FiXs or its Board of Directors which has the effect of rejecting a membership application should not become final without approval by legal counsel.
12. Any FiXs member who has concerns about the propriety under the antitrust laws of any discussion or activity at any FiXs meeting should disassociate himself from any such discussions or activities, leave any meeting if the discussion or activity persists, and report the matter to a FiXs officer and/or FiXs legal counsel.

Membership Policy

FiXs will not:

1. Exclude any entity from FiXs membership unless it fails to satisfy objectively reasonable and neutral membership criteria.
2. Restrict FiXs members from dealing with nonmembers.
3. Limit access to information developed by FiXs, unless such limitation is firmly grounded upon the need to protect trade secrets or other proprietary information.

Topics of Discussion that will be Avoided at FiXs Meetings

1. Current or future prices.
2. What constitutes a “fair” profit level?
3. Possible increases or decreases in prices.
4. Standardization or stabilization of prices.
5. Pricing discounts.
6. Credit terms.
7. Control of sales or levels of output or production.
8. Allocation of markets.

9. Refusal to deal with an entity because of its pricing or distribution practices.
10. Marketing, purchasing, or pricing decisions of individual companies.
11. Whether or not the pricing practices of any industry member are unethical or constitute an unfair trade practice.
12. Individual company bids or intentions to bid for particular products, procedures for responding to bid invitations or specific contractual arrangements.
13. Plans of individual companies concerning the design, characteristics, production, distribution, marketing or introduction dates of particular products, including proposed territories or customers.
14. Discuss or exchange information regarding the above matters during social gatherings incidental to FiXs-sanctioned meetings, even in jest.

These prohibitions highlight only the most basic antitrust principles. Participants in FiXs meetings should consult counsel with respect to specific activities, interpretations or advice.

Conclusion

This policy statement is a general statement of antitrust principles. No policy statement can anticipate every issue that may arise in the course of an organization's activities. FiXs and its members must remain continuously aware of potential antitrust concerns. If any participant has a question about the legality of a proposed activity or course of action, the matter should be immediately referred to the FiXs President who will discuss it with legal counsel. In this manner, FiXs will be able to pursue its legitimate objectives while fully complying with the antitrust laws.

9.0 CONFLICT OF INTEREST POLICY

Article I, Purpose

The purpose of the conflict of interest policy is to protect this tax-exempt organization's (Organization) interest when it is contemplating entering into a transaction or arrangement that might benefit the private interest of an officer or director of the Organization or might result in a possible excess benefit transaction. This policy is intended to supplement but not replace any applicable state and federal laws governing conflict of interest applicable to nonprofit and charitable organizations.

Article II, Definitions

1. Interested Person

Any director, principal officer, or member of a committee with governing board delegated powers, who has a direct or indirect financial interest, as defined below, is an “interested person”.

2. Financial Interest

A person has a financial interest if the person has, directly or indirectly, through business, investment, or family:

- a. An ownership or investment interest in any entity with which the Organization has a transaction or arrangement,
- b. A compensation arrangement with the Organization or with any entity or individual with which the Organization has a transaction or arrangement, or
- c. A potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which the Organization is negotiating a transaction or arrangement.

Compensation includes direct and indirect remuneration as well as gifts or favors that are not insubstantial.

A financial interest is not necessarily a conflict of interest. Under Article III, Section 2, a person who has a financial interest may have a conflict of interest only if the appropriate governing board or committee decides that a conflict of interest exists.

Article III, Procedures

1. Duty to Disclose

In connection with any actual or possible conflict of interest, an interested person must disclose the existence of the financial interest and be given the opportunity to disclose all material facts to the directors and members of committees with governing board delegated powers considering the proposed transaction or arrangement.

2. Determining Whether a Conflict of Interest Exists

After disclosure of the financial interest and all material facts, and after any discussion with the interested person, he/she shall leave the governing board or committee meeting while the determination of a conflict of interest is discussed and voted upon. The remaining board or committee members shall decide if a conflict of interest exists.

3. Procedures for Addressing the Conflict of Interest

- a. An interested person may make a presentation at the governing board or committee meeting, but after the presentation, he/she shall leave the

meeting during the discussion of, and the vote on, the transaction or arrangement involving the possible conflict of interest.

- b. The chairperson of the governing board or committee shall, if appropriate, appoint a disinterested person or committee to investigate alternatives to the proposed transaction or arrangement.
- c. After exercising due diligence, the governing board or committee shall determine whether the Organization can obtain with reasonable efforts a more advantageous transaction or arrangement from a person or entity that would not give rise to a conflict of interest.
- d. If a more advantageous transaction or arrangement is not reasonably possible under circumstances not producing a conflict of interest, the governing board or committee shall determine by a majority vote of the disinterested directors whether the transaction or arrangement is in the Organization's best interest, for its own benefit, and whether it is fair and reasonable. In conformity with the above determination it shall make its decision as to whether to enter into the transaction or arrangement.

4. Violations of the Conflicts of Interest Policy

- a. If the governing board or committee has reasonable cause to believe a member has failed to disclose actual or possible conflicts of interest, it shall inform the member of the basis for such belief and afford the member an opportunity to explain the alleged failure to disclose.
- b. If, after hearing the member's response and after making further investigation as warranted by the circumstances, the governing board or committee determines the member has failed to disclose an actual or possible conflict of interest, it shall take appropriate disciplinary and corrective action.

Article IV Records of Proceedings

The minutes of the governing board and all committees with board delegated powers shall contain:

- a. The names of the persons who disclosed or otherwise were found to have a financial interest in connection with an actual or possible conflict of interest, the nature of the financial interest, any action taken to determine whether a conflict of interest was present, and the governing board's or committee's decision as to whether a conflict of interest in fact existed.
- b. The names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion, including any alternatives to the proposed transaction or arrangement, and a record of any votes taken in connection with the proceedings.

Article V, Compensation

- a. A voting member of the governing board who receives compensation, directly or indirectly, from the Organization for services is precluded from voting on matters pertaining to that member's compensation.
- b. A voting member of any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Organization for services is precluded from voting on matters pertaining to that member's compensation.
- c. No voting member of the governing board or any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Organization, either individually or collectively, is prohibited from providing information to any committee regarding compensation.

Article VI, Annual Statements

Each director, principal officer and member of a committee with governing board delegated powers shall annually sign a statement which affirms such person:

- a. Has received a copy of the conflicts of interest policy,
- b. Has read and understands the policy,
- c. Has agreed to comply with the policy, and
- d. Understands the Organization is charitable and in order to maintain its federal tax exemption it must engage primarily in activities which accomplish one or more of its tax-exempt purposes.

Article VII Periodic Reviews

To ensure the Organization operates in a manner consistent with charitable purposes and does not engage in activities that could jeopardize its tax-exempt status, periodic reviews shall be conducted. The periodic reviews shall, at a minimum, include the following subjects:

- a. Whether compensation arrangements and benefits are reasonable, based on competent survey information, and the result of arm's length bargaining.
- b. Whether partnerships, joint ventures, and arrangements with management organizations conform to the Organization's written policies, are properly recorded, reflect reasonable investment or payments for goods and services, further charitable purposes and do not result in inurement, impermissible private benefit or in an excess benefit transaction.

Article VIII, Use of Outside Experts

When conducting the periodic reviews as provided for in Article VII, the Organization may, but need not, use outside advisors. If outside experts are used, their use shall not relieve the governing board of its responsibility for ensuring periodic reviews are conducted.

10.0 TERMS OF USE OF FIXS INTELLECTUAL PROPERTY AND LICENSING

The FiXs Intellectual Property Policy provides that FiXs may grant designated Members a non-exclusive license to possess and use all or portions of FiXs Intellectual Property. Any possession or use of any FiXs Intellectual Property without a specific license to do so is expressly prohibited.

FiXs expressly authorizes individuals working in support of a FiXs-designated committee, work group, contract or FiXs officially-sanctioned activity a non-exclusive license to use and possess FiXs Intellectual Property solely for the further advancement and/or development of such intellectual property and the objectives of the Federation. All such efforts will be governed by the FiXs Intellectual Property Policy Statement.

Any other use of FiXs Intellectual Property is only authorized under the terms of a separate and individual license or contract. Any such license or contract to use FiXs Intellectual Property shall contain, as a minimum, in addition to any other applicable terms and conditions, the provisions of the FiXs Terms of Use Agreement set forth below.

TERMS OF USE AGREEMENT

THIS TERMS OF USE AGREEMENT (“AGREEMENT”) IS BETWEEN (1) YOU, AS AN INDIVIDUAL CREDENTIAL HOLDER AND/OR THE SPONSOR OR SUBSCRIBING PARTY OF AN INDIVIDUAL CREDENTIAL HOLDER, AS APPLICABLE, AND (2) THE FEDERATION FOR IDENTITY AND CROSS-CREDENTIALING SYSTEMS, INC. (“FIXS”) OR ITS’ AUTHORIZED CREDENTIAL ISSUERS AND SOLUTION PROVIDERS. THIS AGREEMENT APPLIES TO THE USE OF ANY AND ALL FIXS CERTIFIED CREDENTIALS ISSUED BY FIXS OR FIXS AUTHORIZED CREDENTIAL ISSUERS.

BY EITHER SPONSORING THE ISSUANCE OF A FIXS CERTIFIED CREDENTIAL TO AN INDIVIDUAL, OR BEING THE INDIVIDUAL FIXS CERTIFIED CREDENTIAL HOLDER BEING ISSUED A FIXS CERTIFIED CREDENTIAL, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS OF USE, PLEASE CANCEL, RETURN, AND/OR REVOKE, AS APPLICABLE, ANY FIXS CERTIFIED CREDENTIAL ISSUED OR PROPOSED TO BE ISSUED, AND CEASE IMMEDIATELY ANY USE OF SUCH CREDENTIAL.

DEFINITIONS

“FiXs Authorized Solution Provider” or “Credential Issuer” is a FiXs member that issues FiXs Certified Credentials to qualified users for themselves and/or other Sponsors or Subscribing Parties and processes and responds to authentication inquiries.

“FiXs Certified Credential” is an identity credential issued by an approved FiXs Credential Issuer who has contracted to follow the FiXs Trust Model and all corollary policies, rules, guidelines and implementation standards for vetting, enrolling, maintaining, and revoking identity credentials.

“Sponsor” is an organization that uses the services of a Credential Issuer and sponsors Subscribers or other participants to be issued FiXs Certified Credentials.

“Subscriber” or “Subscribing Party” is a member or non-member organization that is a Primary Trusted Organization sponsoring individual users to be issued FiXs Certified Credentials.

“FiXs Intellectual Property” includes, without limitation, all components of the FiXs Network; the FiXs brand, marketing collateral, trademark and other FiXs marks; as well as the FiXs Bylaws; Operating Rules, Trust Model and all governance, operational, security and technical specifications documents.

“FiXs Network” is the end-to-end system comprising the physical infrastructure, operating principles and processes to authenticate FiXs Certified Credentials.

“Licensee” is the individual holder (person) of a FiXs Certified Credential or a Subscribing Party or Sponsor of a Subscribing Party.

SCOPE OF LICENSE

Any and all FiXs Intellectual Property used in the issuance, use, and/ or revocation of a FiXs Certified Credential is licensed, not sold. You may use this FiXs Intellectual Property only as expressly permitted in this Agreement. Your use of any other intellectual property provided by, sold by, or used by any FiXs Authorized Solution Provider or Credential Issuer is subject to the separate terms of use granted by the applicable third party with regard to any such intellectual property that is not FiXs Intellectual Property.

GRANT OF RIGHTS

FiXs grants the individual holder of a FiXs Certified Credential, or Subscribing Party, (in each instance, a “Licensee”), as applicable, the non-exclusive, non-transferable, revocable, limited right to use the FiXs Intellectual Property for the sole purposes of identity authentication within, across, and between components of the FiXs Network.

LIMITATIONS AND RESTRICTIONS

The Licensee may not manipulate, alter, change, or create derivative works of FiXs Intellectual Property. Licensee shall not reverse engineer, decompile or disassemble any FiXs Intellectual Property. The Licensee shall only use any FiXs trademark or service mark as expressly authorized to do so.

The Licensee shall adhere to the applicable Operating Rules, Policies, Security Guidelines and other FiXs or third party procedures for the issuance, use, and revocation of FiXs Certified Credentials.

PRIVACY

The Subscribing Party agrees to comply with the FiXs Privacy Policy Statement which is incorporated in full in this Terms of Use Agreement and included herewith.

GOVERNING LAW

Within the United States

This Agreement, and its enforcement and construction, shall be governed in all respects by the laws of the Commonwealth of Virginia (excluding its conflicts of law principles) for all FiXs Certified Credentials issued in or used in the United States or its territories.

Outside of the United States

For all FiXs Certified Credentials issued and used outside of the United States, the laws of the applicable country of issuance and use shall apply to the extent that they conflict with the laws of the Commonwealth of Virginia, U.S.A (excluding its conflicts of law principles).

PERFORMANCE STANDARDS AND WARRANTY

FiXs requires certain minimum performance standards to govern the work to be performed by FiXs Authorized Solution Providers or Credential Issuers. Such performance standards have been promulgated by FiXs by written agreement between FiXs and the FiXs Authorized Solution Provider or Credential Issuer, as applicable.

Each FiXs Authorized Solution Provider or Credential Issuer warrants that its performance hereunder shall conform in all material aspects with such performance standards, and shall provide that if such Solution Provider or Credential Issuer's performance hereunder shall, at any time during the term of this Agreement, fail to conform in all material aspects with such performance standards, it shall correct such non-conforming performance at its sole cost and expense.

LIMITATION OF LIABILITY

FIXS AND ANY FIXS AUTHORIZED SOLUTION PROVIDER OR CREDENTIAL ISSUER SHALL NOT, IN ANY EVENT, BE LIABLE IN CONNECTION WITH ANY ASPECT OF FIXS CERTIFIED CREDENTIAL (E.G., WITHOUT LIMITATION, ISSUANCE OF, REVOCATION OF, CANCELLATION OF, USE OF, OR FAILURE TO DO ANY OF THE FOREGOING WITH RESPECT TO, A FIXS CERTIFIED CREDENTIAL) FOR SPECIAL, INDIRECT, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST INCOME, LOST REVENUE, OR LOST PROFIT, WHETHER SUCH DAMAGES WERE FORESEEABLE OR NOT AT THE TIME THAT THIS AGREEMENT WAS ENTERED INTO.

THE SUBSCRIBING PARTY, SPONSOR, OR INDIVIDUAL FIXS CERTIFIED CREDENTIAL HOLDER, AS APPLICABLE, SHALL DEFEND, INDEMNIFY, AND HOLD HARMLESS FIXS, ITS OFFICERS, DIRECTORS, EMPLOYEES, CONTRACTORS AND AGENTS, FROM AND AGAINST ALL LIABILITIES, DAMAGES, EXPENSES, TO INCLUDE REASONABLE ATTORNEYS FEES, FINES, AND CLAIMS OF ANY KIND OR BASED ON ANY LEGAL THEORY, ARISING FROM THE ISSUANCE OF, REVOCATION OF, CANCELLATION OF, USE OF, OR FAILURE TO DO ANY OF THE FOREGOING WITH RESPECT TO, A FIXS CERTIFIED CREDENTIAL.

SEVERABILITY

In case any one or more of the provisions in this Agreement shall, for any reason, be held to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability shall not affect any other provisions of this Agreement, and this Agreement shall be construed as if such invalid, illegal or unenforceable provision was and is not contained in this Agreement.

MODIFICATION OR AMENDMENT

This Agreement may be modified by FiXs from time to time as deemed necessary in the sole discretion of FiXs, and Licensee's continued use of a FiXs Certified Credential after such modification will be deemed to be Licensee's agreement to such modified Agreement.

ENTIRE AGREEMENT

The Agreement constitutes the complete agreement between FiXs and Licensee as to its subject matter, and supersedes any and all written and oral communications or agreements previously existing as to this subject matter.

11.0 Brand, Trademark, and Graphics Policy

Article I. Purpose and Introduction

The purpose of this Policy is to promulgate formal standards for the usage of the brands and trademarks of the Federation for Identity and Cross-Credentialing Systems, Inc. ("FiXs" or the "Federation"). It is recognized that increasing customer awareness of FiXs

and FiXs-related offerings is an important market differentiator as well as vital for preservation and protection of the intellectual property assets and property rights of the Federation.

This market awareness and recognition requires consistent usage, presentation, and communication.

Article II. Application and Limitations on Use

Any form of reference to the Federation for Identity and Cross-Credentialing Systems, Inc.; the Federation for Identity and Cross-Credentialing Systems; or FiXs; may be made subject to the limitations set forth in this policy.

Specifically, companies or organizations who maintain membership in “good standing” under the provisions of the Bylaws of the Federation may make use of the FiXs brand and/or trademarks indicating their membership in the Federation consistent with the provisions of this policy.

Further, member organizations that may deploy FiXs-certified or duly authorized service offerings utilizing the FiXs Network or its related attributes or features may indicate that they are a “FiXs-Certified Solution Provider”, a “FiXs-Certified Service Provider”, deploying a “FiXs-Certified Credential”, or “FiXs Credential” meaning that they are deploying some form of FiXs-Certified capability, offering, or feature. The specific terminology to be used will be subject to the specific use case under which the member organization has been affirmatively certified or authorized by FiXs for usage. Only duly authorized FiXs solution or service providers may use the designation that they are FiXs-Certified; deploying any form of “FiXs-Certified” solution or service; deploying a FiXs-Certified Credential, or doing anything under the auspices of FiXs .

Any member organization of the Federation who has NOT been duly certified or authorized to have, use, or provide access to the FiXs Network, FiXs-based solutions, services or any related attributes, or credentials is expressly prohibited from making any implicit or explicit statements to the effect that they have or provide any form of FiXs-Certified solutions, services, credentials or attributes thereof.

For purposes of clarity, maintaining a membership in the Federation DOES NOT entitle any organization or company to assert or imply in any manner that they are, have been, or provide anything certified, authorized, prepared under the auspices of, or in accordance with the Federation or FiXs, nor does membership in and of itself provide any form of endorsement by the Federation or FiXs.

Article III. Brand Mark and Trademark Uses

Increasing customer and market awareness of the Federation, FiXs, and or related offerings requires absolute consistency in all forms of print and electronic media; to include descriptions in all service offerings, proposals, marketing materials, and signage on products and service components. It is also imperative that any oral communications

of these forms of reference are used consistent with the same usage in other forms of expression.

1. Use of FiXs Brand Names, Marks and Trademarks – The use of FiXs Brand Names, Marks, and Trademarks must appear prominently, consistently, legibly, and accurately and match in color when possible and at the size, color, and frequency parity when described in all forms of documents or text, in written and electronic format. When used as signage, as an “emblem” or “logo”, or on other artifacts, or as part of a service being provided or advertised, FiXs Brand Marks and Trademarks must appear prominently, consistently, legibly, and accurately and match in color when possible and at the size, color, and frequency parity.
2. Use of the FiXs Brand Marks and Trademarks with Other Marks – When used with other brand marks, the FiXs Brand Marks and Trademarks must appear prominently, consistently, legibly, and accurately and match in color when possible and at the size, color, and frequency parity comparable to FiXs participation or representation in the specific use.
3. Depicting FiXs Brand Names or Trademarks on Identity Cards and/or Credentials – All “actual” or “sample” identity cards or credentials must display the entire Brand Mark or Trademark in a clearly legible manner and at least at the same size, color, and frequency parity with other systems or network-related brand marks or trademarks shown on the card or credential.
4. Use of Correct and Consistent Language – The use of the correct and consistent terminology when referring to FiXs, FiXs Names or Trademarks throughout and in all forms of communications is an essential aspect of this Policy.

Article IV. Using Our Brand Names and Trademark(s)

The full name(s) of the Federation for Identity and Cross-Credentialing Systems, Inc. must be used at least once in all communications that refer to the Federation, FiXs, membership in FiXs, or FiXs-certified offerings, products and/or services. It is desirable that this depiction be used at the point of “first use” of any reference to the Federation.

1. Using Uppercase and Lowercase Letters – When using the full name of the Federation, or the Federation for Identity and Cross-Credentialing Systems, Inc., the trademark should be distinguished from surrounding text by at least using Initial Capital Letters, such that the “F”, “I”, “C”, “C”, “S”, and “I” always appear in uppercase. Usage of the full name of the Federation may also be portrayed in ALL CAPITAL LETTERS; **Bold Letters**, *Italic Letters*, “In Quotes”, or in stylized form.

When using the abbreviated form of reference to the Federation, or “FiXs”, the mark should be distinguished from surrounding text by at least Capital Letters for the “F” and the “X” with the other letters, “i” and “s” in lowercase. Usage of the term FiXs may also

be portrayed on ALL CAPITAL LETTERS; **Bold Letters**, *Italic Letters*, “In Quotes”, or in stylized form.

The term “and” or the symbol “&” may be used interchangeably in referring to the full name of the Federation.

2. Using Brand Names or Trademarks as Adjectives – The term “FiXs” may be used as an adjective, as in “FiXs-Certified Credential”, or “FiXs-Certified Solution Provider”, “FiXs-Service Provider” or other such form of adjectival reference. At a minimum, the Brand Name(s) or Trademark(s) must be used as adjectives in their first or most prominent mention subsequent to any use in the title, headline or cover page of any communication.
3. Usage of the Trademark Symbols – The “®” and/or “™” trademark symbols, or their local law equivalents, always should appear after the first or most prominent use of the FiXs Brand name(s)
4. Usage with Other Brand Names or “marks” – In all communications the FiXs Brand Names and Trademarks always must be presented with prominence and frequency equal to that of all other system or network related brand names, trademarks or “marks”.
5. Brand Name Translation – The Brand Names and Trademarks of the Federation may appear only in English and not be translated into other languages nor appear in another alphabet.

Article V. Using Correct Language

Using correct and consistent language in all communications is essential for the effectiveness of this policy.

1. Referring to the FiXs Network – All references to the network deployed and operated by FiXs must be referred to as the “FiXs Network”
2. Referring to FiXs Solutions, Services, Processes or Technologies – All references to solutions, services, processes or technologies that are related solely to the instantiation of FiXs intellectual property shall be used with, and as a prefix to, the name of the service or feature being utilized or deployed. The applicable trademark symbols must be used with such usage. Where a authorized service provider may be providing solutions, services, processes or technologies that are utilizing any FiXs intellectual property, the provider may apply its’ own branding applicable to the circumstances; however, clear and legible acknowledgement must be provided and accompanying marks provided indicating that an underlying component is FiXs intellectual property. (i.e. such as the “powered by Intel” mark prevalent in industry).

Article VI. Use in Advertising, Proposals, and Other Forms of Print or Electronic Media

This Policy shall be consistently applied and adhered to in any and all proposals, marketing collateral and brochures, presentation materials, contractual documents, advertisements, informational documents and any other formats in any form, whether printed or electronic, to include on or over the Internet, as well as in oral communications as applicable.

Article VII. Use at the Point of Interaction

A card or credential holder's first visual indication of the availability to use or have FiXs-Certified Credentials utilized may be as exterior signage, but it is also important to display such signage at the point of interaction as well as on any enrollment device or authentication device, as applicable.

Article VIII. Use in Depicting Cards or Card Communications

When depicting the FiXs credential or card in visual format or on the actual card, the card "format" or "topology" shall be consistent with the technical specification requirements set forth for the card "type", security level, or other attributes required by the usage case and consistent with the specifications set forth by the Federation. In all cases, the FiXs trademark shall be present in a clearly visible manner on one or more sides of any such card. In cases where the only one side is depicted in visual format or representation (i.e. in print), the FiXs trademark shall be present in a clearly visible manner on the representative card.

Article IX. Use on Signage

When displaying the FiXs Brand Mark or Trademark, the "mark" shall be displayed horizontally and in an easily recognizable manner.

Article X. Brand and Trademark Specifications

Brand marks are generally used to represent the brands on cards, products, and services and to promote the brand through advertising and marketing.

The current Brand and Trademarks of the Federation are:

"Federation for Identity and Cross-Credentialing Systems, Inc. ®";

And,

"FiXs®",

And,



The Brand Marks and Trademarks are reflected visually on the FiXs website, on all FiXs documents, and are available from the FiXs Administrative Staff at the request of a FiXs member in “good standing”.

FiXs Brand Marks may be provided to non-members for specific uses; such as marketing, advertising, trade events, publications, and other such uses on a case-by-case basis at the sole and explicit authorization of an officer of the Federation.

Article XI. Specific Examples of “Do’s” and “Don’ts”

Provided below are examples of “Do’s” and “Don’ts” as it relates to Brand Names and Trademarks.

“Do’s” Include:

1. Distinguish trademarks from surrounding text by at least using:

Initial Capital Letters
ALL CAPITAL LETTERS

Bold Letters

Italic Letters

“In Quotes”

In stylized form or logo

2. Use proper trademark form and spelling

3. Use trademarks with the generic product and/or services descriptor, e.g.:

FiXs Network

FiXs Certified Credentials

FiXs Authentication Station

FiXs Credential Issuer, etc.

“Don’ts” Include:

1. Don’t hide trademarks within other text,

E.g. “Use the fixs network to authenticate fixs credential holders”

2. Don’t purposely misspell trademarks,

E.g. FiXs

F I X S

Fed. For ID X-Credentialing Sys.

3. Don’t use alone as a generic product name,

E.g. FIXS

4. Don't use as a noun,

E.g. Use FIXS to gain access

5. Don't use a plural form of trademark,

E.g. FIXSs
FIXSes

6. Don't make trademarks possessive,

E.g. FIXS's
FIXS'
Federation for Identity and Cross-Credentialing Systems'

7. Don't use trademarks as verbs,

E.g. I am/will FIXSing your identity

8. Don't use alternative spellings or acronyms,

E.g. FICS
FICCS

Article XII. Violations of this Policy and Enforcement

Adherence to and compliance with this Policy is of significant imperative to promote and protect the market position of the Federation as well as the value of FiXs intellectual property and assets. Maintaining and ensuring compliance with this Policy is a fundamental responsibility of executing the business plan and day-to-day operation of the Federation. It is the intention of this Policy to actively manage and enforce the provisions herein.

Protection, defense, and enforcement measures for violations of this Policy shall be considered through all practical and legal means, to include all legal and financial remedies as well as injunctive relief.

Article XIII. Filing of Applications for Trademark, Patents and Other Legal Protections

A fundamental component of executing the business plan and the successful business operations of the Federation shall entail applying for and obtaining, as possible, the

relevant trademark, patent and other legal protections for Federation property and assets, as applicable.

12.0 DISASTER RECOVERY

The purpose of this Disaster Recovery Policy is to set forth the measures that have been made or will be activated in the event of a “disaster”, which is essentially any event, man-made or naturally incurring, that may attempt to destroy or otherwise impair the continuity of operations the Federation and the FiXs Network. This policy addresses the personnel, processes, technological, and operational aspects of the Federation.

Personnel (Officer) Continuity

Consistent with the Bylaws of the Federation, the Vice President of the Federation will act in the absence or unavailability of the President in the event of a “disaster”. The Corporate Secretary and the Treasurer of the Federation shall maintain the ability to serve in the capacity of the other in the event of a disaster and the incapacitation or unavailability of the other.

The organizational delegation of authority shall flow from the President, to the Vice President, to the Secretary, then to the Treasurer of the Federation. Should all of the officers be in some manner incapacitated, a majority of the then available Founding Members shall appoint designated successors to such officers until such time that the “disaster” situation is stabilized, whereupon the full Board of Directors can attain a quorum and appoint permanent replacements consistent with the Bylaws.

Organizational and Membership Continuity

The Federation will maintain complete and current documentation of all governance policies, to include: without limitation, the Trust Model; Operating Rules; Implementation Guidelines; Technical Specifications; contact lists of all officers, members, Federation service providers and contractors, and government counterparts and sponsors; contracts; licenses; financial/tax information and records; membership list including membership level and status; and all current records of the Federation. A duplicate copy in electronic format (i.e. CD, thumb drive, etc.) of such records will be provided to each current officer of the Federation for safeguarding and use in the case of a disaster situation. The “safeguarding” officer shall appropriately protect and not access, distribute, or otherwise allow the “opening” of such records except in the case of a bonafide disaster as determined by the then available Founding Members of the Federation.

Technical and Operational Continuity

The contractor providing laboratory management services for the Federation will provide, as determined by the Federation, the “failover” site for maintaining continuity of operations of the FiXs Network components and continuity of operations.

The laboratory management services contractor shall also maintain a current copy of all versions of the software code, technical specification, documentation, and other assets to

provide continuity of the core FiXs Network components such as the FiXs TGB and interface specifications. Such assets shall only be disclosed as directed by the acting officer then in charge of the Federation in the event of a disaster.

The service providers maintaining the respective data stores of the federated credential holder personal information data sets shall have their own Disaster Recovery Policy that shall be implemented to maintain continuity of operations in the event of a disaster affecting their ongoing operations. This policy and its' ability to be deployed in a timely manner are subject to periodic review and audit by the Federation.

The tertiary components of the FiXs Network, such as the authentication station providers; credential issuers, investigative services, etc. shall implement disaster recovery plans consistent with the service requirements of their respective service clients.

Periodic Disaster Recovery Plan Exercise

This Disaster Recovery Plan will undergo a "test exercise" of its basic tenants and ability to respond in case of a disaster situation on no less than an annual basis. The findings of such exercise shall be reported to the Board of Directors upon compilation of such findings as part of its' routine operational forum.

Violations of this Policy

Any violations of this Policy, to include but not limited to the violation of ensuring proper protection and non-disclosure of "safeguarded" information, shall result in the termination of offending parties' relationship with the Federation, at the discretion of the President, in addition to any other remedies at law, regulation, or otherwise.

Note: For FiXs Definitions/Terminology, see [Master Glossary of Terms/Definitions](#)