Version: 0.1 2012-02-22	The status of this document is "initial release for comment" and the process of iteration will be in collaboration with the IDcubed.org Model Trust Framework project advisory team.
1. Business Rules	
1.1 Scope and Application	These System Rules apply to Participants in the use of the Personal Data Locker System. Addenda 2 defines key words and phrases. All Policies incorporated by reference shall have the same force and effect as if their terms and provisions were literally and explicitly included within these System Rules.
1.2 Roles	A Party may conduct more than one Role. A Party is bound to the rights and duties defined for a given Role by execution of a Participation Agreement, or, in the case of the Policy Authority or System Operator, based upon other means including but not limited to bylaws, operating agreements, patent license or other means.
1.2.1 Policy Authority	The Policy Authority is the Participant that is responsible for promulgating these System Rules and Policies and for governance of the Personal Data Locker System. The Policy Authority designates the Party that conducts the Role of the System Operator, and delegates such authority to the System Operator as may be necessary to manage the Personal Data Locker System while retaining oversight and governance.
1.2.2 System Operator	The System Operator is the Participant Responsible for day to day management and operations of the Personal Data Locker System and is accountable to the Policy Authority and the Principal Users for
1.2.3 Principal User	A Principal User is a Participant that has been Enrolled and Registered in the Personal Data Locker System. The Principal User shares, by their permission, Personally Identifiable Information for transmission to, storage in, quantification by and sharing through the Personal Data Locker System. The Principal User transmits Personally Identifiable Information, including behavioral, location and other data to the Personal Data Locker System through web-based systems and a mobile device that has been linked to that Principal User during their Enrollment and Registration, or subsequently. It is axiomatic to these System Rules and the purpose of the Personal Data Locker System that the Principal User owns and controls the use and sharing of their Personally Identifiable Information existing or that has existed in the Personal Data Locker System.
1.2.4 Observer User	An Observer User is a Participant that has been Enrolled and Registered in the Personal Data Locker System and who is also authorized by one or more Principal Users to view designated parts of such Principal User's Personally Identified Information.
1.2.5 External Application or Service Provider	An External Application or Service Provider is a Participant that has provided an Application or a Service being used by or within as part of the Personal Data Locker System, in accordance with the Information Security and Internal Controls Policy, the Accreditation and Certification Policy and that complies with the API and Developer Specifications Policy.
1.3 Management	The day to day management and decision making related to the Personal Data Locker System shall be conducted by the System Operator on behalf of the Policy Authority in accordance with these System Rules.

1.3.1 Enrollment and Onboarding	The System Operator is responsible for enrollment and registration of each Party conducting one or more Roles under these System Rules, in compliance with the Enrollment and Registration Policy. The Enrollment and Registration Policy shall include the process of identity proofing each applicant, ensuring asset by each applicant to the Participation Agreement, account creation, provisioning relevant services and system configurations, and linking the relevant mobile device to the account.
1.3.2 Maintaining FAQ, Forum and Help Desk Support	The System Operator shall make available and maintain an up to date FAQ and an online topic based discussion forum where Participants may share information about and discuss functionality and use of the Personal Data Locker System. A Forum accessible only to Principal Users shall be offered and managed by the System Operator. The System Operator shall make available to Principal Users a help desk function enabling each such Participant to request help with use of the Personal Data Locker System, by online chat, e-mail, telephone or other means.
1.4 Suspension and Termination	
1.4.1 Reports or Suspicion of Non-Compliance With System Rules	
1.4.2 Investigation and Report by System Operator	
1.4.3 Recourse	
1.4.3.1 Warning	
1.4.3.2 Audit	
1.4.3.3 Suspension	
1.4.3.4 Termination	
1.4.3.5 Reinstatement	
2. Legal Rules	
2.2 Participation Agreements	
2.2.1 Party's Must Assent to Participation Agreement	Every Party conducting one or more Roles in the Personal Data Locker System must Assent to the Participation Agreement for each such Role. The System Operator shall ensure that each Participation Agreement binds the Party signing it to the Role or Roles that Party will conduct under these System Rules, and ensure the binding is legally enforceable.
2.2.2 Principal User Participation Agreement	Every Principal User must Assent to the Principal User Participation Agreement as a precondition to account registration. Minimally, the Principal User Participation Agreement shall describe the Personal Information that will be collected or used by the Personal Data Locker System and the purposes for the collection or use.
2.2.3 Observer User Participation Agreement	Every Observer User must Assent to the Observer User Participation Agreement as a precondition to account registration.
2.2.4 Reserved.	
2.2.5 Reserved.	

2.3 Personal Information Ownership and Control	
2.3.1 Personal Information and Identity Account Ownership	
2.3.1.1 Personal Information Ownership by Principal User	The Principal User owns and controls access to, use, modification, copying, derivative works and redaction or deletion of the data they enter into Personal Data Locker System, including, without limitation, data entered based upon sensor signals passively collected from the Principal User's mobile phone and also including, without limitation, audio, text or survey responses input actively by the Principal User.
2.3.1.2 Identity Account Ownership by by Principal User	The Principal User owns their identity account, and may request a full export of the information comprising their account including any identifiers, private encryption keys authenticating the account, contact information contained in the account related to the Principal User, notes in the account, and any log files related to the history of the account or use or access to the account. The Principal User may cause their identity account to be deleted upon termination of their Participation in the Personal Data Locker System. Deletion of the Identity Account may occur after a reasonable grace period, to be noted in the Principal User Participation Agreement and not to exceed 25 business days.
2.3.2 System Information and Non-Principal User Account Ownership	Subject to Section 2.3.1 inclusive of all subsections, the Policy Authority owns or is deemed to own all information and other data in the Personal Data Locker System, including any account it may host to facilitate access by Observer Users or other Non-Principal Users, and all logging data, reporting data, processing data or other data or information.
2.4 Rights and Responsibilities Related to Information	
2.4.1 Information Licensing and Sharing Rules	
2.4.1.1 Principal User License and Permissions	Each Principal User shall permit the System Operator and such other Participants as the Principal User shall authorize, to access explicitly defined data elements of their Personal Information according to the Personal Information License Terms Policy.
2.4.1.2 Policy Authority License and Authorization	The Policy Authority directly or acting through the System Operator, shall provide one or more licenses whereby other Participants may access and use the Personal Data Locker System that is consistent with the terms of these System Rules. Assent to said license shall be accomplished as part of the assent to the Participation Agreement by Principal Users.
2.4.2 Fair Information Rules	The following Fair Information Rules are intended, and shall be construed, to afford the Principal User the rights associated with ownership of their Personally Identifiable Information transmitted to or existing within the Personal Data Locker System.

2.4.2.1 Transparency	The Policy Authority shall be transparent and notify Principal Users regarding collection, use, dissemination, and maintenance of personally identifiable information.
2.4.2.2 Individual Participation	
2.4.2.2.1 Principal User Involvement	The Policy Authority shall involve Principal Users in the process of using their own PII collected within the Personal Data Locker System.
2.4.2.2.2 Principal User Consent and Informed Consent	The Policy Authority shall receive each Principal User's Consent for the collection, use, dissemination, and maintenance of their PII and shall receive each Principal User's Informed Consent when such PII is behavioral or health related.
2.4.2.2.3 Principal User Access, Correction and Redress	
2.4.2.2.3.1 Mechanisms for Data Request and Communication	The Policy Authority shall provide mechanisms to each Principal User for appropriate access, correction, and redress regarding use of their PII. The aforementioned mechanisms shall include means to enable each Principal User to request all data relating to them and to have that data communicated to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonably accessible and intelligible manner and form.
2.4.2.2.3.2 Reasons for Denial	The Policy Authority shall give the reason(s) why a request made under Section Section 2.4.2.2.3.1 is denied.
2.4.2.3 Purpose Specification	The Policy Authority shall specifically articulate the authority, whether based upon contract, license, civil, military or other authority, that permits the collection of PII of a Principal User and specifically articulate the purpose or purposes for which such PII shall be used.
2.4.2.4 Data Minimization	The Policy Authority shall only collect PII or a Principal User that is directly relevant and necessary to accomplish the specified purposes of these System Rules and only retain such PII for as long as is necessary to fulfill such specified purposes.
2.4.2.5 Use Limitation:	The Policy Authority shall use PII of a Principal User solely for the purposes specified in these Principal User Participation Agreement. Sharing PII shall only occur in accordance with the terms of the Principal User Participation Agreement.
2.4.2.6 Data Quality and Integrity	The Policy Authority shall ensure that PII of a Principal User is accurate, relevant, timely, and complete.
2.4.2.7 Security	The Policy Authority shall protect PII of a Principal User (in all media) through appropriate security safeguards against the risk of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
2.4.2.8 Accountability and Auditing	The Policy Authority shall be accountable for complying with the Rules of Section 2.4.2 governing Fair Information Rules, inclusive of all subsections, and for providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these Rules and all applicable privacy protection requirements.
2.5 Liability	
2.5.1 Disclaimers	

2.5.2 Limitation of Liability	No Principal User shall bear any liability to the Policy Authority or System Operator for any acts or omissions, to the extent only that the Principal User acted in compliance with all applicable terms of these System Rules. However, nothing in the immediately prior sentence shall limit the liability of a Principal User for acts or omissions that constituted gross negligence or recklessness for for which a civil or criminal remedy exists. Neither the Policy Authority nor the System Operator shall bear any liability to any Principal User for any acts or omissions, to the extent only that the Policy Authority and/or System Operator acted in compliance with all applicable terms of these System Rules. However, nothing in the immediately prior sentence shall limit the liability of a Policy Authority and/or System Operator for acts or omissions that constituted gross negligence or recklessness for for which a civil or criminal remedy exists.
2.5.3 Limitation of Damages	
2.6 Dispute Resolution	
2.7 Notices	
2.8 Survival	
2.9 Amendment	Amendment of these System Rules shall comply with the terms and provisions of the Amendment and Change Management Policy.
3. Technology Rules	
3.1 Use Cases and Supported Services	
3.2 Information Security	
3.3 Standards, Profiles and Configurations	
3.4 API and Developer Requirements	
3.5 Change Management	
Addeda 1: Formal Policies Incorporated by Reference	
Pol-1: Participation Agreements	
Pol-2: Enrollment and Registration	
Pol-3: Amendment and Change Management	Link [Draft in Progress]
Pol-4: Fair Information Rules	Link [Draft in Progress]
Pol-5: API and Developer Specifications	Link [Draft in Progress]

Pol-6: Information Security and Internal Controls	Link [Draft in Progress]
Pol-7: Personal Information License Terms	Link [Draft in Progress]
Pol-8: Reserved	
Pol-9: Reserved	
Pol-10: Reserved	
Pol-11: Reserved	
Pol-12: Accreditation and Certification	Link [Draft in Progress]
Pol-13: Logging, Record Keeping and Audit	Link [Draft in Progress]
Pol-14: Exception and Waiver Request	Link [Draft in Progress]
Pol-15: Appeal Request	Link [Draft in Progress]
Pol-16: Dispute Resolution	Link [Draft in Progress]
Pol-17: Antitrust Policy	Link [Draft in Progress]
Pol-18: Trust Mark License	Link [Draft in Progress]
Pol-19: Creative Commons	Link [To Selected CC URL]
Addenda 2: Defined Terms and Glossary	
Addenda 3: Interlateral Codification of Legal and Technology Rules	
Addenda 4: General Commentary	
Attribution and Credits:	This information was drafted by Dazza Greenwood of CIVICS.com and is being iterated for general use as part of a Model Trust Framework project in collaboration with the IDcubed.org in partnership with John Clippinger and MIT Professor Sandy Pentland. More information on this project is available at: http://civics.com/model-trust-framework The eventual Model Trust Framework is intended to have several reference implementations, including for B2B (e.g. Supply Chain, Partner Ventures, Industry SSO, etc) B2C (eCommerce, eLearning, etc) G2C (eGovernment, Open Government, eDemocracy, etc) and this Personal Data Trust Framework.
Copyright:	