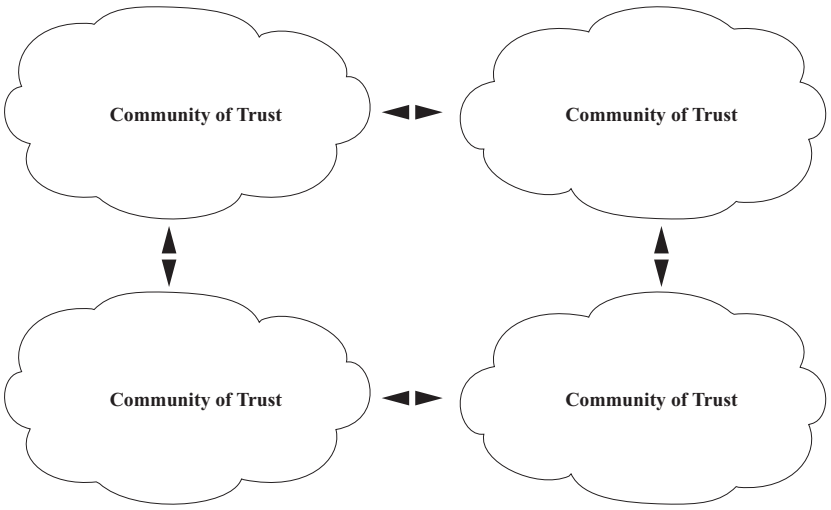
Community of Trust™

Reprivata, Corp.

OVERVIEW

The implementation of *Community of Trust* provides the Chief Executive Officer or Director of an organization with a simple Cyber Risk Management tool similar to tools currently used to manage the financial condition of an organization or enterprise. *Master Agreements* similar to those used in financial settlement mechanisms are implemented to manage all aspects of the organization's cyber risks. This standardized contract structure also enables cyber insurance underwriters to price risk more effectively and efficiently enabling your enterprise or organization to obtain efficiently priced and effective cyber insurance. Community of Trust also enables uniform interoperability between communities that enables the interconnection to or with other Communities of Trust using the NIST Cyber Security Framework as a governance mechanism.



Overview A Community of Trust Service is a governance structure that uses policies, procedures, contracts and technology approaches to create a more secure environment for all interconnected parties to conduct business or access information. The Community of Trust Owner has a direct legal relationship and logical IP network connection with an employee, their third party interconnected entities and other end users. The legal and policy layer of a Community of Trust provides a uniform and repeatable definition of how connected parties will conduct business. This includes meeting cybersecurity threshold standards, providing enforcement mechanisms, enabling uniform insurance underwriting and limiting liabilities between those connected to the network. The technical component of an implementation of a Community of Trust is defined by the individual Community of Trust Owner as required to become U.S. Cybersecurity Framework (CSF) Tier 3 Compliant. There is no technical specification or mandated product or service requirements.

U.S. Cybersecurity Framework (CSF) Community of Trust enables *Comprehensible* Cybersecurity Framework (CSF) deployment where there is alignment of expectations and incentives among Community of Trust owners, its insurers, its interconnected entities, its end users and its employees. Designing and implementing durable enterprise or nation-state cyber protection is complex. Community of Trust deployments ease this transition by implementing a *Standard Contract Structure* and enabling the enterprise or nation-state to define and extend their risk management policies to those who are interconnected with their Community of Trust and enables interoperability with other Community of Trust Owners.

A Community of Trust is a Practical Implementation of the U.S. Cybersecurity Framework (CSF). In 2013, US Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity,* called for the development of a voluntary risk-based cybersecurity framework (CSF) that is "prioritized, flexible, repeatable, performance-based, and cost-effective." The Cybersecurity Framework (CSF) Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. It is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk.

What is the justification to and executive or a director of public and private organization for using the CSF as the basis for a Community of Trust?

Adoption of Community of Trust.org means:

1) Showing "you are paying attention" to cybersecurity in general.
2) Showing the regulators "you are paying attention".
3) Showing your customers "you are paying attention".
4) Showing your shareholder/investors and the financial markets that "you are paying attention".
5) Community of Trust is "one stop shopping" when seeking to restore customer confidence, investor protection and market stability in the face of cyber terrorism, hacktivism and cyber crime.

Community of Trust provides a "Sarbanes Oxley" approach to certification of the public and private organization's compliance with CSF guidance to obtain cyber insurance, among other things. This requires Officer of the company or organization to certify compliance with the guidance.

The CSF defines Tier 3 in the following manner:

> ***Risk Management Process*** The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
>
> ***Integrated Risk Management Program*** There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
>
> ***External Participation*** The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

The **Cybersecurity Framework Core** covers these basic concepts:

> ***Identify*** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
>
> ***Protect*** Develop and implement the appropriate safeguards to ensure delivery of CNI services.
>
> ***Detect*** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
>
> ***Respond*** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
>
> ***Recover*** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

An organization self analyzes and certifies that they meet the Cybersecurity Framework Tier 3 status or acquires their own Community of Trust from an authorized Community of Trust Service Provider. They must drive the CSF Tier 3 framework and adoption to all those who interconnect with them or they will not be able to certify they meet the Cybersecurity Framework Tier 3 status. (e.g. If they allow a non-certified entity to Interconnect with them.) Community of Trust Owners benefit from the *Cybersecurity Insurance* industry's development of standards, procedures, and other measures that comprise the CSF and their endorsement of this standard. Members of Community of Trust enter into a contract with the Community of Trust to certify compliance with the specification *(As derived from the CSF)* that sets forth minimum standards and requirements for guarding against cyber security threats and the handling of personally identifiable information (PII).

Among other things a, Community of Trust Owner must:

1) Nominate a qualified Cybersecurity Risk Control Officer to be accountable for the implementation of the Community of Trust.

2) This executive level position will communicate the mission priorities, available resources, and overall risk tolerance to Critical Infrastructure (CI) leadership.

3) The implementation, monitoring and audit of the business/process level will be the responsibility of the Community of Trust Risk Control Officer.

4) The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile.

5) The implementation/operations level communicates the Profile implementation progress to the business/process level.

6) The business/process level uses this information to perform an impact assessment.

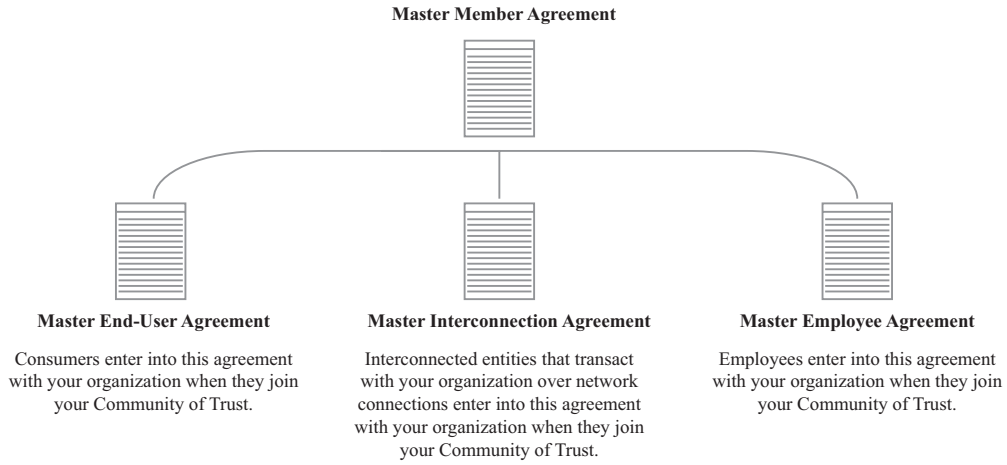
7) Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization’s overall risk management process and to the implementation/operations level for awareness of business impact.

Technology A Community of Trust may use off the shelf, Underwriter Laboratories UL CAP 2900 certified technology provided by Community of Trust or from multiple vendors which cover multiple sources to be able to qualify as a Tier 3 Community of Trust. They may also choose to use multi-layered encryption technology as needed to secure edge devices on their network and capture traffic outbound to cyber attackers within their encrypted core. The Members have access and the right to use this technology as a function of being a member of Community of Trust.

Once the legal and policy layer is implemented the only thing that remains is for the Owner of a Community of Trust to follow the Tier 3 requirement to constantly asses, test and verify the policies, processes and technology is being implemented and followed sufficiently to maintain the Tier 3 status. This may include the use of the technology provided to a Member by Community of Trust or may be implemented by the Community of Trust Service Provider as a part of the service.

2017 Master Agreements Community of Trust requires that an organization become a member to obtain access to the Master Agreements that constitute and enable an independent Community of Trust instance. These agreements are comprised of a *2017 Master Membership Agreement* that requires members to organize and deploy their independent Communities of Trust using a process that will facilitate the reliable implementation of security policy and technical interoperability between independent Communities of Trusts and interconnected entities. *The 2017 Master Interconnection Agreement*, similar to a financial settlement mechanism, requires that the Community of Trust Owner and all interconnected entities enter into an agreement that requires a minimum threshold of Cyber Insurance and that each party be named as an additional insured in the policy. It also requires the counterparty to be U.S. Cybersecurity Framework (CSF) Tier 3 compliant. The *2017 Master End User Agreement* enables an organization to provide a standardized agreement with customers that mitigates risk and creates a trusted (PII) relationship between customers and the Community of Trust owner. The *2017 Master Employee Agreement* enables an organization to provide a standardized agreement with employees that mitigates risk and creates a trusted (PII) relationship and removes ambiguity in the relationship with the employer and/or the Community of Trust owner. The *2017 Master Member Agreement* with a *Service Provider Addendum* enables an organization to contract with a third party to implement the Community of Trust policy and technical layer. It is a contract between a Community of Trust Service Provider and a Community of Trust Owner.

Reprivata Community of Trust

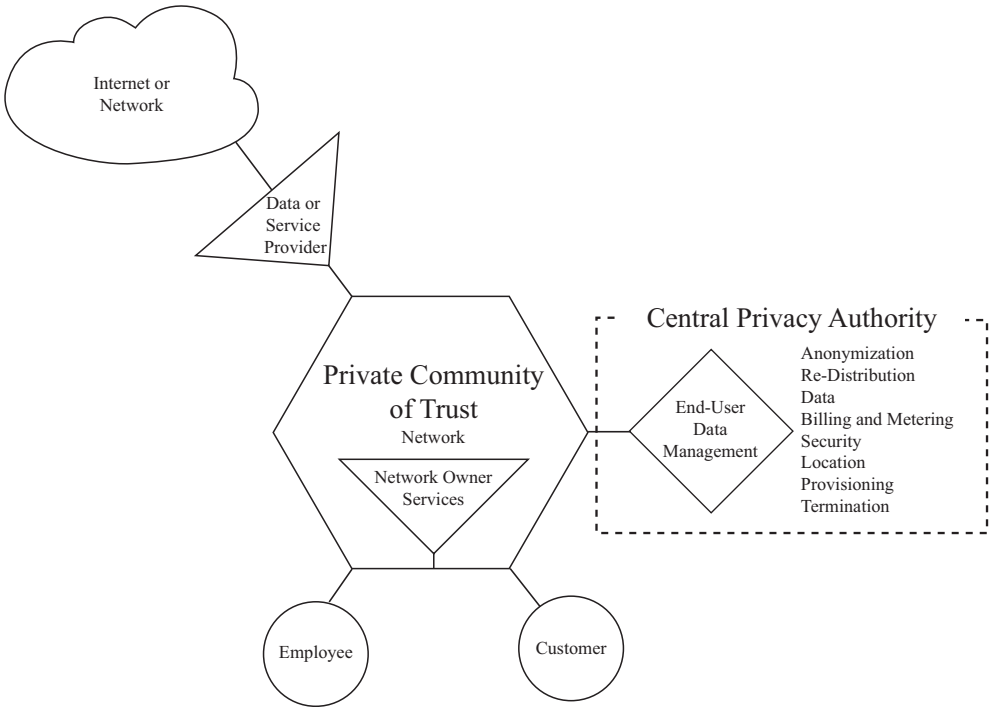


A Community of Trust Owner/Operator will use any or all three of the primary Master Agreements with end users, customers, employees or third party interconnected entities that connect to the Community of Trust. These contracts define a repeatable and identifiable methodology and process of how to become secure and maintain Tier 3 according to the U.S. Cybersecurity Framework (CSF).

Background In 2014 Reprivata, Corp. provided the first Community of Trust Service offering to a select group of users. This enabled Reprivata to understand the functions needed for a Community of Trust. Reprivata implemented technology to build and operate a Community of Trust using a specific suite of software for the end users, employees and third parties to connect in a secure manner. Reprivata is the founding member of Community of Trust, which is an organization that defines and promotes this unique approach to providing cybersecurity, limiting liabilities and re-privatizing individual and corporate privacy via the new set of agreements and policy defined as a Community of Trust.

Community of Trust Concepts A Community of Trust is defined as a Policy and Legal layer combined with content and applications delivered via an IP network to the authorized connected entities of the Community of Trust. The Community of Trust includes a group of end users, employees and third party connected entities that have a need to access content, applications and communications network services via public, private (or a hybrid of both) types of networks from any edge device (ie: desktop computers, notebook computers, tablets of any OS or smart phones of any OS or any IP connected device). The Community of Trust Owner agrees to a legal and policy layer and that they meet U.S. Cybersecurity Framework Tier 3 status and obtain cyber insurance for the entirety of their Community of Trust. The Community of Trust services could be provided to the end users who are interconnected to the core network directly or they could be provided by Internet Protocol Enabled Services (IPES) that are accessible through the Community of Trust closed network and defined as “the Services”. Each third Party interconnected entity has also agreed to meet U.S. Cybersecurity Framework Tier 3 status and obtain cyber insurance as a requirement of being a part of the Community of Trust. A Community of Trust will also require the IPES to accept communications from the Community of Trust Owner as a proxy for the end user and agree to only track or gather the PII and/or the Non-PII from the end user that the end user has agreed to share (if any), pursuant to the end user’s Community of Trust profile.

Reprivata Community of Trust



A Community of Trust Service Provider is defined as the entity that provides process and technology to create a secure Community of Trust using the U.S. Cybersecurity Framework (CSF) to meet or exceed the requirements of Tier 3 in the CSF.

Community of Trust has a broad interpretation of cyber security both in terms of what cybersecurity is and how it impacts public and private sector entities. Community of Trust believes the Global Visibility of all TCP/UDP/IP addresses on all of the approximately 3 billion IP connected devices is fundamentally flawed from a cybersecurity perspective. This enables any entity to attack any other entity with millions of computers from anywhere in the world. The attack surface on the Internet is so large the cyber criminals are able to do what they want to whom ever they want from anywhere. Community of Trust believes the risk of being attacked is so large that there is a strong need to become more vigilant and explore different approaches to become more secure as an organization. Organizations now understand that it is essential to maintain a high level of network security with all interconnected parties. Community of Trust provides a comprehendible and achievable road map to reach this goal.

The Community of Trust agreements define that the Cybersecurity Framework (CSF) Tier 3 is the minimum standard that must be met to interconnect with end users, employees or third party networks. It requires the Community of Trust Owner and third party connected entities to obtain and maintain cyber insurance to interconnect with each other to ensure the risk associated with interconnection is both limited and distribute among the interconnected parties. Community of Trust Service Providers may implement a suite of software as a component to the total network solution for a Community of Trust.

Community of Trust believes there must be simultaneous efforts on multiple fronts for the cyber security issues that exist today to be managed and dealt with in a uniform, repeatable and consistent manner. The three areas that must be worked simultaneously are as follows:

1) Policy (Agreements designed to drive uniform behavior between two or more connected parties)
2) Process (Consistent use of Business and Technical Policies to insure overall alignment to business Risks between two or more connected parties)
3) Technology (Enables the Policies and the Processes to achieve specific Risk Goals)

Community of Trust Membership The Member requirements are defined in the Community of Trust Member Agreement which explains how a member would join, what the organization would provide to the members and what the member is expected to do and provide as a Community of Trust Owner. The Member can be a Community of Trust Owner and provide the Community of Trust for themselves or can contract with a Community of Trust Service Provider Member to obtain a secure networking environment.

There are 3 kinds of Community of Trust Members.

1) Community of Trust Owners who have a direct relationship via the contracts with their Employees, End User Consumers and Third Party connected entities.
2) An Insurance Provider who will provide Cyber Insurance to the Community of Trust Owners
3) A Community of Trust Service Provider who will provide Communities of Trust to Community of Trust Members who want to own their own a Community of Trust but do not want to implement the infrastructure needed to enable a Community of Trust.