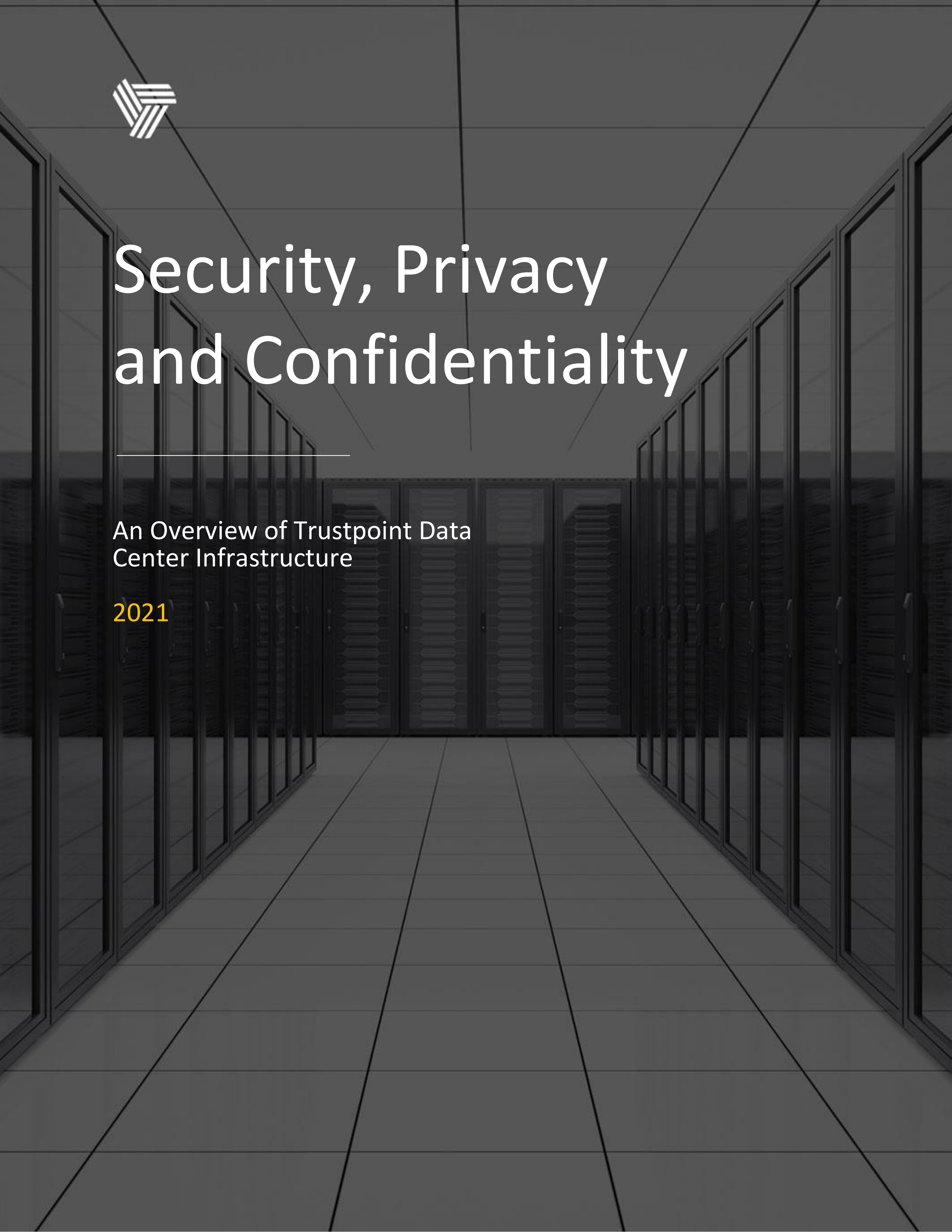

Security, Privacy and Confidentiality

An Overview of Trustpoint Data Center Infrastructure

2021

Security Overview

Trustpoint One(TP1) employs multiple approaches to ensure conflict and confidentiality integrity. With an active internal network between all client-facing employees, each client matter is carefully vetted to ensure no conflicts of interest. TP1 augments this intensive vetting with security and policy layers to ensure both active and passive protection measures in the areas of security and privacy. These additional layers include but are not limited to:

Physical Security: Our TP1 production environment is serviced by two geographically separated secure data centers with strict, limited and controlled access to the various premises. Implemented security measures and policies within our operational facilities restrict individual vetted access to areas of need for specific job requirements. All other areas are physically restricted via authentication methods, including assigned keycards, private Personal Identification Numbers (PIN) and biometrics. Datacenter access requires all three of these methods for entry. While on-premise, non-IT personnel are escorted and monitored personally within the key areas to provide necessary oversight. CCTV monitoring and recording is also in use within specific areas, with recording activated by movement or sound. Data Center cages and cabinets remain locked unless in use and specific areas are restricted to IT personnel based on maintenance requirements.

Network Security is of utmost importance and includes numerous security measures and design features to protect our environment from unauthorized access. Security measures includes our decision to deploy industry-standard solutions for routers, firewalls and data transport providers with multiple layers of security. The combined design provides a secure environment for data operations with additional security restrictions with the file system encoded in the application layer of our software. All data center network links are secured and redundant with auto-failover for reliability, resiliency and redundancy. Network communications between offices are secured via MPLS-VPN links maintaining no visibility from the public internet.

Security Policies have been developed to meet the high standards of our business and the clients of which we serve. The implemented standards are regularly tested through methods such as internal and external audits, penetration tests and executive procedural reviews and IT requests for enhancements. The combined design produces an environment and team focused on the elimination of security risks.

Storage Policies specify that critical data retained on TP1 storage solutions utilize encryption methodology to reduce access risk. Internal policies also limit access to such areas to those with required approval. Steps have also been taken to separate client data from business requirements to create a segregated environment. This is frequently a dedicated environment to specific clients within each data center per client agreements.

Data Transport Policies have been implemented to ensure that business and client data and communications are securely transferred via industry standards. TP1 supports most common methods of secure data transmission leveraging multi-factor, as well as hosting internal options to directly connect and transfer data between organizations. These methods include ShareFile and onsite dedicated FTP servers utilizing industry standard data security protocols (SSL). As a baseline, all data is transferred under AES 256 encryption standards and transmissions must be compliant with TP1's data transmission policy. For non-electronic transfer of data, encrypted hard drives are supported with the restriction that the delivery meets specific security measures.

Hosting Application Policies provide further levels of security which are integrated into our environment to continue the hardening of the platforms used to access our hosted applications. The standard of SSL VPN with MFA connectivity is a requirement for external user access to our environments/applications. Once connected, Group Policies (GPO) further secure the user to the applied security standards. The specific case requirements occur through a standard effort as client administrators closely work with the TP1 client services team to secure their environment as needed.

Access Control and Monitoring is critical for operational success and security and TP1 understands this need. One of our main focuses is to identify occurrences within and external to our environment which might impact service delivery. The requirement is to know who is requesting what info/access and what is delivered as part of that request/access. TP1 utilizes multiple solutions as we continually monitor our environment. We analyze our circuits, networking infrastructure (routers, firewalls, ports, switches) and servers for concerns. Critical application servers (SQL, Web, Email, Active Directory, Backup, Terminal Services and servers dedicated for customer use) report ongoing data and security logs against thresholds to quickly alert team members of items of concern for needed actions.

These integrity and security elements, supported by our internal and external privacy policies, represent TP1's holistic approach to data protection.

Data Center Specifications

TP1 utilizes two data centers to support the TP1 business operations and provide secure technology services and solutions to our clients.

The first data center is co-located in the Flexential Alpharetta Georgia Data Center and the second one is co-located within a Databank facility in Denver Colorado. Both facilities provide High Availability (HA) capabilities for solutions such as our Relativity Hosting platforms and dedicated environments for clients. Physical security measures include 4-zone security access, biometric scanners and monitored security cameras and intercom systems. These sites are compliant with several industry and regulatory standards to match and further supplement Trustpoint audit reports.

Both locations are connected via dedicated high-speed links and serve as backups to the other location as a mirrored data center.   Both centers are designed with redundancy of power (including generators), HVACs, data circuit providers, and monitoring on a 24x7x365 standard by dedicated engineering teams.

TP1 computing systems are designed from the ground up and deployed on custom-built hardware utilizing various technologies such as disk mirroring and RAID technologies to protect the data that we host and manage. Our server designs are based on an active-active sync capable platform to further strengthen our solutions. Data protection of production systems includes implementations of solutions and processes such as direct backups, replication, syncing and snapshots to meet the varying requirements of data priority and client needs.

Industry Certification Highlights and Specifics

TP1 conducts independent audits on an annual basis for:

- SOC 2 Type II
- ISO 27001:SSAE 18
- HIPAA (2017)
- EU-US Privacy Sheild Framework

Flexential Alpharetta and Databank Denver compliance includes but not limited to:

- PCI DSS compliant site
- Annual, independent audits according to:
    - EU-US Privacy Shield framework
    - SOC 1 Type II, SOC 2 Type II, SOC 3
    - HIPAA
    - ISO 27001:SSAE 18

Following SOC guidelines, we have in place a comprehensive set of policies, procedures and plans that cover Disaster Recovery, Business Interruption Analysis, and Business Continuity. Created in 2009, these are continually maintained, tested, and regularly reviewed as part of a bi-annual process to evolve our solutions as needed to continue to provide the best and most secure products. This includes planning for pandemics and weather emergencies. Please note that emergency recovery solutions and planning are also available for our clients if desired.

About Trustpoint One

Trustpoint One helps clients address business and legal challenges associated with the discovery and review of electronically stored information with legal technologies and services for law firms, corporations and governments. Founded in 2008 and based in Atlanta, GA, Trustpoint's end-to-end eDiscovery services include forensic collections, processing, analytics, predictive coding and managed review and are supported from ten national offices and nine national review centers.

To learn more about Trustpoint, contact us via email at info@trustpoint.one, via phone at 1.855.669.1205, or on the web at www.trustpoint.one.