DATA SECURITY POLICIES & CONTROLS
An Overview for Customers and other External Parties

PrimeTrust
## DATA SECURITY POLICIES & CONTROLS

<table>
<thead>
<tr>
<th>Security Policy Overview</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Access and Transmission Policies</td>
<td>2</td>
</tr>
<tr>
<td>Change Management</td>
<td>3</td>
</tr>
<tr>
<td>Incident Response</td>
<td>4</td>
</tr>
<tr>
<td>Transaction Processing</td>
<td>5-7</td>
</tr>
<tr>
<td>Customer Data</td>
<td>8-11</td>
</tr>
</tbody>
</table>
The security of our clients’ sensitive data is the lifeblood of our business at Prime Trust. **Prime Trust takes data security seriously**, both when the data is in transit to and from various services and when the data is at rest in our servers. Prime Trust uses bank level encryption on all connections when receiving and sending data and all data is stored securely in our encrypted cloud.

We contract an independent third-party security firm to run penetration testing regularly and Prime Trust is proud to report that no critical vulnerabilities have ever been identified. We also conduct third-party security audits and are 5002 certified. In addition, Prime Trust has never experienced a data breach.

Our policies and procedures are grounded in fundamental logic and practicality. Where possible and practical, we employ best-practices, generally enforced by technology, corporate policy and management oversight.

We review our policies and procedures regularly. We may from time to time change our security policies and practices by enhancing them or by simplify them, generally without making any public announcement.
Prime Trust employs only domestic US, full-time engineers who are required to perform the majority of their work on site in our office headquarters. As a matter of firm policy, we do not hire off-shore engineers. All engineers and operational staff are required to submit to detailed background checks as a condition of employment.

All Prime Trust employees, including our engineers, are required to comply with information security protocols, including the use of strong passwords on all devices used to conduct firm business. Access to production systems, including databases, is restricted to our Head of Engineering and principal engineer. All production system activities are captured and subject to audit by the Chief Technology Officer.

Access to Prime Trust dashboards and other operational user interfaces is tightly controlled by credentials that include a unique User ID and strong password combination for every user. Prime Trust employees are prohibited from sharing passwords with anyone for any reason and will never ask a client to share his or her password. Access passwords are stored encrypted in the system’s database; if a password is lost it must be reset to a temporary password by a system administrator; temporary passwords must be changed immediately upon the user’s next logon. When an employee is terminated or leaves the firm, his or her system access is terminated as part of Prime Trust’s employee off-boarding procedure. Employee access and entitlements to Prime Trust’s user interfaces are reviewed and adjusted accordingly each quarter by the Chief Technology Officer.

Prime Trust employees are strictly prohibited by policy from downloading and transmitting by email or other unsecured mechanism any report or other data generated by Prime Trust’s platform for any reason. Any collateral containing proprietary or personally identifiable information (“PII”) must be transmitted using a secure mechanism only as defined in Prime Trust’s internal policies.

As a condition of interacting with PrimeTrust’s systems, all employees are trained in PII handling and data security.
Prime Trust maintains strict development and QA / testing cycles and supporting documentation to ensure that new feature development and rollout does not negatively impact our customers.

**CHANGE MANAGEMENT**

Prime Trust will notify clients in advance of any planned disruption in service due to system maintenance. Routine maintenance windows are generally outside of normal business hours to minimize any disruption to our clients.

We do not generally share our testing or development schedule, or any supporting documentation with our clients.

Prime Trust will, from time to time, release new features and bug-fixes to its customers without making a prior announcement. The Prime Trust Product group periodically releases product notes and news, which contain information detailing bug fixes and enhancements shortly after they are released to production. These communications are generally included in an email to our customer contact(s) of record and are also posted to the Prime Trust.com product blog.

While we don't publish a public product roadmap, Prime Trust customers are welcome to request information about our upcoming features and development milestones to help them plan for what’s coming.
INCIDENT RESPONSE

Prime Trust maintains a disaster recovery and communication plan that is designed to be enacted in the event of a major catastrophe or system failure or data breach which results in our inability to service our customers.

Each situation is different and therefore can only be evaluated in real-time; the Chief Technology Officer, Head of Product, and Head of Engineering will be responsible for evaluating the specific situation; if practical, they will convene with the Chief Executive Officer and determine what communication is required, and what steps will be taken to restore our platform’s security and functionality.

Safeguarding customer data is our top priority; if we detect or suspect a data breach, we may shut down, disable access to, or otherwise immobilize our platform, which may affect our customers’ ability to conduct business. We may or may not make any announcement to our customers apprising them of the situation.

Once our team can establish the security and integrity of customer data, we will bring the system online again as soon as practically possible.
TRANSACTION PROCESSING

Transaction processing refers to the technical elements associated with the movement of funds in customer accounts. Funds are typically moved in one of four ways: eCheck/ACH, Credit Card, Wire Transfer, and Paper Check.

WHAT DATA IS COLLECTED?

In addition to the customer PII ("Personally Identifiable Information", detailed below), Prime Trust collects additional data based on the customer’s chosen payment method. The data is collected and transmitted only over connections that are secured by financial industry standard bank level SSL/TLS encryption. Specific data elements are detailed below.

ACH/ECHECK

For incoming or outgoing funds, Prime Trust collects:

- Accountholder’s Name
- Account Number
- Bank Routing Number
- Account Type (Checking/Savings, Business/Personal)

CHECK

For incoming checks, no data is collected as funds are pushed from customers to Prime Trust. For outgoing checks, the following data is collected:

- Name on the Account
- Mailing Address
TRANSACTION PROCESSING

CREDIT CARD
Credit card information is never handled by Prime Trust. In our mobile, API and dashboard systems, customers enter their credit card details into a form presented by our payments processing partner, Worldpay. Worldpay is among the world’s largest payments processors, completing more than 40 billion transactions annually. Investor credit card data is stored only by Worldpay in their PCI compliant environment. Worldpay collects the following data:

- Accountholder’s Name
- Account Number
- Bank Routing Number
- Account Type (Checking/Savings, Business/Personal)

In our API environment, the merchant (typically the issuer) integrates into the credit card processor directly. The data then passes from the merchant to the processor and Prime Trust never touches the data.

WIRE TRANSFER
For incoming wires, no data is collected as funds are pushed from customers to Prime Trust. For outgoing wires, the following data is collected:

- Name on the Account
- Account Number
- Routing Number
WHAT DATA IS COLLECTED?

With the exception of credit cards, where no data is stored by Prime Trust, all the collected data is stored in a Prime Trust’s encrypted cloud. Access to the data is limited exclusively to Prime Trust and its bank partners through our secure administration portal. The administration portal is permissioned only for employees who require access to the data and features advanced security features such as expiring login sessions, strong password requirements, and bank level encryption. All employees who require access to the data are subject to pre-employment detailed background checks, and all such employees receive regular continuing education in the handling of sensitive data.

WHAT DOES PRIME TRUST DO WITH THE DATA?

Prime Trust shares transaction data with its banking partners. Account information is transmitted to banks over their secure interfaces to enact the movement of funds. Prime Trust stores the data in perpetuity in the event of an audit, fraud investigation, and/or court orders for the data. Where necessary, data may be provided to government agencies upon request.
CUSTOMER DATA

Customer data refers to PII provided by customers about themselves at the time of submission, which can include but is not limited to: name, residence address, email address, tax ID number, and date of birth. Prime Trust collects and stores this customer information for the purposes of banking compliance including anti-money laundering, communications, and capitalization table management including the secure transmission of customer data to an issuer’s SEC Registered Transfer agent, upon an issuer’s request.
WHAT DATA IS COLLECTED?

The data collected will depend on the services being performed by Prime Trust and/or its banking partners, along with the vehicle through which the customer chose to send us data. The data is collected and transmitted only over connections secured with bank level data encryption. Specifics are detailed below:

NATURAL PERSONS

For natural persons, Prime Trust collects:

- Full Name
- Country
- Address
- Email
- Phone Number
- Tax ID Number
- DOB

COMPANY

For companies, Prime Trust collects:

COMPANY’S

- Name
- Country
- Address
- Email
- Phone Number
- Tax ID Number
- State of Formation

AUTHORIZED PERSONS’

- Full Name
- Country
- Address
- Email
- Phone Number
- Tax ID Number
- DOB
TRUSTS

For trusts, Prime Trust collects:

**TRUST’S**
- Name
- Country
- Address
- Email
- Phone Number
- Tax ID Number
- State of Formation

**AUTHORIZED PERSONS’**
- Full Name
- Country
- Address
- Email
- Phone Number
- Tax ID Number
- DOB

RETIREMENT ACCOUNT

For retirement accounts such as self-direct IRAs and 401(k)s, Prime Trust collects:

**RETIREMENT ACCOUNT’S**
- Name
- Company’s Country
- Company’s Address
- Contact Email
- Contact Phone Number
- Tax ID Number
- State of Formation

**AUTHORIZED PERSONS’**
- Full Name
- Country
- Address
- Email
- Phone Number
- Tax ID Number
- DOB
WHAT DATA IS STORED?

All the collected data is stored by Prime Trust in our encrypted cloud.

WHAT DOES PRIME TRUST DO WITH THE DATA?

Access to the data is tightly controlled and limited only to authorized Prime Trust employees, select vendors and API Integrated partners, and any related broker-dealers, exchanges, investment advisors or other agents of a customer, through Prime Trust’s secure administration portal and over Prime Trust’s encrypted API. Prime Trust’s vendors vary based on the services being used, however they typically include bank depository partners, compliance accountants and auditors, and SEC registered Transfer Agents. Prime Trust stores the data in perpetuity in the event of an audit, fraud investigation, or requests for the data from law enforcement agencies or regulatory bodies.