Clera Information Security Policy

Purpose & Scope: This Information Security Policy outlines how **Clera** protects sensitive data and systems in its fintech platform. It covers compliance obligations, handling of personal and financial data, access control, cloud infrastructure security, monitoring and incident response, remote work security, and third-party vendor management. All team members and systems at Clera must adhere to these policies to safeguard user bank account and investment information.

1. Regulatory Compliance

Clera is committed to complying with all relevant data protection laws and industry security standards applicable to fintech firms handling personal identifiable information (PII) and financial data. We integrate compliance into our operations to protect user privacy and meet partner requirements (including Plaid's due diligence standards). Key compliance measures include:

- **GDPR (EU General Data Protection Regulation):** Clera abides by GDPR requirements for any personal data of EU residents . We obtain explicit user consent for data access via Plaid/Alpaca, use data only for stated purposes, and uphold individuals' rights (access, correction, deletion). Personal data is processed lawfully, minimized to what is necessary, and stored no longer than needed for the service. If a data subject requests their information be deleted or exported, Clera will promptly comply in accordance with GDPR timelines.
- **CCPA (California Consumer Privacy Act):** For California residents, Clera honors all CCPA rights . Users can request disclosure of what personal data we have collected and ask for deletion of that data. We do **not** "sell" user personal information; if this policy ever changes, we will provide a "Do Not Sell My Info" opt-out as required. Clera responds to verified consumer requests within statutory deadlines and extends similar privacy rights to all users for transparency and fairness.
- **SOC 2 Type II:** We are aligning our controls with the AICPA SOC 2 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy. SOC 2 is an internationally adopted framework ensuring that service organizations securely manage customer data to protect privacy . Clera maintains documented security policies and procedures, conducts regular risk assessments, and will pursue an independent SOC 2 Type II audit to demonstrate our effective controls.
- **ISO/IEC 27001:** Clera is building an Information Security Management System (ISMS) in line with ISO 27001 standards . ISO 27001 provides a systematic framework for managing sensitive company and customer information securely, including risk management, staff training, and continuous improvement of security controls. By following ISO 27001, we ensure our security practices remain comprehensive and up to date. We will consider obtaining certification as the company grows to formally attest to our security program's maturity.
- **Other Regulations & Standards:** We monitor and comply with other applicable laws and guidelines. For instance, we follow data breach notification laws (GDPR's 72-hour notice rule, California's requirements, etc.), and ensure our policies meet the due

diligence expectations of partners like Plaid and Alpaca (both of whom maintain high security standards, such as ISO 27001 and SOC 2 compliance). We also consider emerging regulations in fintech (e.g. PSD2, DORA in the EU) to stay ahead of requirements for secure open banking integrations.

2. Data Handling and Protection

Clera enforces strict controls over how sensitive user data is collected, stored, processed, and transmitted. This includes users' bank account linking data (via Plaid), investment portfolio data (via Alpaca), login credentials, API keys, and any PII. Our data handling practices ensure confidentiality and integrity at all times:

- **No Plaintext Credentials:** Clera never stores users' bank or brokerage login passwords in any form. During bank account linking, users enter credentials directly through Plaid's secure interface – we do not see or store those credentials . Plaid provides us with secure tokens, not raw passwords, so we avoid liability of holding banking login info. Similarly, for Alpaca connections, users authorize via API keys or OAuth tokens; Clera treats those as secrets and does not retain any plaintext password.
- **Secure Storage of API Tokens:** Any access tokens or keys obtained for integrating with Plaid or Alpaca are stored only on our backend in a secure, access-controlled database . Tokens are **never** exposed on the client side or in logs. We encrypt these tokens at rest (using strong encryption) and restrict database access to the minimal set of backend services that need them. By storing API keys securely and never on user devices, we mitigate the risk of token theft.
- **Encryption of Sensitive Data:** All sensitive data managed by Clera is encrypted both at rest and in transit. We use strong encryption algorithms (AES-256) to protect stored data, and TLS 1.2+ for all network communications . For example, any PII (names, email addresses, account numbers) or financial details are stored in encrypted form in our databases and storage buckets. Likewise, data exchanged with Plaid, Alpaca, and between our front-end and backend is always sent over HTTPS (TLS) connections. This ensures that even if data were intercepted or accessed without authorization, it would be unreadable.
- **Data Minimization & Masking:** We adhere to the principle of collecting and retaining only the minimum data necessary to provide our service. The Plaid API is used to retrieve account and routing numbers and transaction data needed for Clera's features – we request only the scopes/data that our application requires, and nothing more. Any particularly sensitive information (e.g. full account numbers or balances) is masked in our system displays unless absolutely required. For instance, we might store only the last 4 digits of an account number for identification, while the full number remains encrypted or only available through Plaid's tokenized calls.
- **Access Control on Data:** Internally, we classify user data (e.g. public, internal, confidential, highly sensitive) and apply controls accordingly. PII and financial data are classified as highly sensitive and are accessible only by back-end services and authorized personnel with a business need (such as a limited number of engineers or support staff). Even within our systems, service-to-service access to sensitive data is

authenticated and logged. Direct database queries on tables containing PII require elevated privileges. This ensures that even within Clera, only the right components and people can handle decrypted sensitive information.

- **Secure Processing & Disposal:** When handling sensitive data in memory or during processing, we take care to avoid exposing it. Our application code avoids writing secrets or PII to logs or debug output. Temporary files, if any, are stored in secure locations and deleted immediately after use. We have secure deletion processes for retiring any storage media that contained sensitive data (using AWS's disk destruction for cloud storage, etc.). Moreover, if a user disconnects their bank or investment account from Clera, we honor that by securely erasing the associated tokens and fetched data after fulfilling any regulatory retention requirements. In compliance with privacy laws, we also delete user data upon account closure or valid user requests, ensuring no residual personal data remains on our systems beyond the retention period.
- **Data Integrity and Backup:** We protect the integrity and availability of user data through regular backups and checks. All production databases are backed up on a scheduled basis to encrypted storage. Backup files are encrypted and stored in a separate, secure location (AWS backup services) with access controls. We periodically test restoring from backups to verify data integrity and our disaster recovery process. These backups ensure that in the event of data loss or corruption, we can restore critical user data with minimal disruption.

3. Access Controls and Identity Management

We enforce strict access controls to ensure that only authorized individuals and systems can access sensitive systems or data. Clera's access control policy is built on the principles of least privilege and robust authentication, in order to reduce the risk of unauthorized access. Key controls include:

- **Multi-Factor Authentication (MFA):** All access to Clera's internal systems (admin dashboards, production infrastructure, databases, etc.) requires MFA for user logins. This applies to engineers, administrators, and any employee accounts with access to sensitive resources. By requiring a second factor (such as an authenticator app code or hardware token) in addition to password, we greatly strengthen account security – use of MFA makes accounts *99% less likely* to be hacked compared to password-only logins . We enforce MFA at the identity provider or VPN level so that even if credentials are phished, an attacker cannot access our systems without the second factor.
- **Strong Authentication Practices:** In addition to MFA, Clera uses industry-standard authentication protections. Passwords (where used) must be strong (complex and unique), and are stored as salted cryptographic hashes. We integrate Single Sign-On (SSO) for our internal tools where possible, so that user access can be centrally managed and monitored. Login attempts are rate-limited to prevent brute force, and default admin accounts or unused credentials are disabled. For cloud infrastructure access (AWS console, etc.), MFA and hardware security keys are enforced. All API keys or secrets for third-party services are stored securely and rotated periodically to limit exposure.

- **Role-Based Access Control (RBAC):** We implement RBAC to ensure each employee or service has access only to what they need for their role. Each user is assigned roles (or groups) with predefined permissions. For example, a customer support agent might have read-only access to certain account data necessary to assist users, but not to system configuration or raw credentials. Developers have access to development and testing environments, but only a small on-call engineering team can access production systems. This way, we limit exposure of sensitive data to essential personnel only. The **principle of least privilege** is enforced: users and applications are granted access only to the data and operations required for their jobs , and no more.
- **Periodic Access Reviews:** We conduct regular reviews of user accounts and privileges. At least quarterly, the Security Officer (or designated team) reviews all employee and service accounts to ensure permissions align with current job responsibilities. Any access that is no longer needed (e.g., a role change or project completion) is revoked. We maintain an access control matrix mapping roles to permissions to help in these audits. Additionally, when an employee leaves the company or a contractor's engagement ends, we have a rapid deprovisioning process to revoke all access (GitHub, AWS, databases, etc.) immediately. These reviews and revocations prevent privilege creep and ensure our RBAC remains tight.
- **Segregation of Duties:** Clera's processes are designed so that sensitive operations require approval or involvement from multiple authorized persons, preventing any single individual from having unchecked control. For instance, code changes to security-critical modules require peer review and CI/CD approval; production data access may require a ticket and manager approval. We separate duties between development, testing, and operational environments. Admin rights in production are limited and actions are logged (so any misuse can be traced). This segregation reduces the risk of insider threats and accidents by adding checks and balances.
- **Logging of Access:** All privileged access to systems (such as administrative login to servers, database queries on sensitive data, or use of production credentials) is logged in detail. We use centralized logging to record who accessed what and when. These logs are monitored and audited (see **Monitoring** section) to detect any unauthorized or inappropriate access. Users are made aware that their access is monitored as a security measure. Logging deters misuse and helps quickly pinpoint the cause if an incident occurs.

4. Infrastructure Security (AWS & Cloudflare)

Clera's application and data are hosted on cloud infrastructure (primarily Amazon Web Services) with Cloudflare providing network edge security. We follow cloud security best practices to harden our infrastructure, including encryption, firewalls, and secure API communications. Our infrastructure security approach covers:

- **Secure Cloud Configuration (AWS):** We deploy our backend on AWS with a secure-by-design configuration. Each server instance, container, and database in AWS is configured with the principle of least privilege in mind (minimal IAM roles and security group permissions). AWS Identity and Access Management (IAM) policies are tightly

scoped – for example, our application servers can only access the specific S3 buckets or DB tables they require. AWS recommends using identity, resource, and network access controls together with encryption , and we implement all these layers. Security Groups (virtual firewalls) are used to restrict network traffic: only necessary ports (e.g., HTTPS/443) are open to the internet, and internal service ports are isolated within our VPC. Administrative access to AWS management consoles or EC2 instances is limited to specific IPs (or via VPN) and requires MFA (as noted in Access Controls). We also regularly apply patches and updates to our cloud VMs and containers, using AWS Manager and automated patching for known vulnerabilities.

- **Data Encryption (At-Rest & In-Transit):** Clera ensures that all data is encrypted at rest in our AWS infrastructure and in transit across networks. For data at rest, we leverage AWS Key Management Service (KMS) to manage encryption keys and enable encryption on all storage: databases (RDS or DynamoDB) are encrypted with AES-256, S3 buckets have default encryption enabled, and EBS volumes for servers are encrypted . Access to encryption keys is strictly controlled by IAM roles, providing an additional logical separation of data from key access. For data in transit, we enforce TLS encryption end-to-end. All external traffic goes through HTTPS (TLS 1.2+/SSL) – our API endpoints and web frontend are only accessible via **https://** URLs, and we use HSTS headers to prevent downgrade to HTTP. Similarly, any integration calls to Plaid or Alpaca's APIs use their HTTPS endpoints. This dual encryption (at-rest and in-transit) aligns with industry best practices and ensures that sensitive information (bank balances, portfolio details, PII) cannot be read if intercepted or accessed improperly.
- **Cloudflare Web Security:** We use Cloudflare as a content delivery network (CDN) and Web Application Firewall (WAF) in front of our application. Cloudflare terminates HTTPS for our domain, ensuring fast, encrypted connections with modern TLS settings , and caches static content to improve performance for users. Security benefits of Cloudflare include DDoS protection and traffic filtering at the edge: Cloudflare's network automatically mitigates denial-of-service attacks and blocks malicious traffic before it reaches our AWS servers. We have enabled Cloudflare's WAF rulesets to detect and block common web attacks (SQL injection, XSS, etc.) on our application API. We also use Cloudflare Access policies for certain internal admin tools, adding SSO/MFA at the edge. Firewall rules are configured both at Cloudflare (to allow only legitimate app traffic) and at AWS (security groups allowing Cloudflare IP ranges), creating multiple layers of defense. This layered approach means an attacker must get through Cloudflare's protections and then AWS's network controls before ever targeting our app – significantly enhancing security.
- **Secure APIs and Communication:** All communication between Clera's components and with third-party services is secured. Our microservices within AWS communicate over an encrypted internal network or via TLS even internally when possible. We authenticate all API calls between services using tokens or AWS IAM roles so that only authorized calls are accepted. External webhooks (like Plaid webhooks for transaction updates) are verified via signatures or secret keys to ensure they truly originate from Plaid and have not been tampered with. We also sign our outgoing requests where required. In short, every integration point is secured to prevent man-in-the-middle,

spoofing, or unauthorized access. Additionally, we follow secure coding practices for APIs (input validation, proper error handling that doesn't leak sensitive info, etc.) to harden our application itself against attacks.

- **Monitoring and Patching:** Our infrastructure is continuously monitored for vulnerabilities or misconfigurations. We utilize AWS security services (such as Amazon GuardDuty for threat detection and Amazon Inspector for vulnerability scanning) to get alerts on any suspicious activities or known security issues in our environment. System logs and CloudTrail events are collected for analysis (see Monitoring section). We apply critical security patches to OS, containers, and libraries in a timely manner, using an automated pipeline where possible. Configuration changes to cloud resources are tracked via Infrastructure as Code (Terraform) and code-reviewed to catch security-impacting changes. We also enforce that any new cloud service or resource follows our tagging and configuration standards (for example, any new S3 bucket must have versioning and encryption enabled by policy). By staying vigilant and proactive with monitoring and patching, we reduce the window of exposure for new threats.
- **Backup and Disaster Recovery:** Clera's AWS infrastructure is architected with resilience in mind. We perform regular backups of databases and critical data stores, and store those backups securely in a different AWS region. Backups are encrypted and retained according to our data retention policy. We have tested restoration procedures to ensure we can recover from scenarios like data corruption or accidental deletion . In addition to backups, we utilize AWS's high-availability features: for example, databases may run in multi-AZ mode, and our application servers are in auto-scaling groups across multiple availability zones for redundancy. We maintain an Incident Response playbook for major outages (see below) that includes steps for spinning up replacement infrastructure from code if needed. Our goal is to be able to recover quickly and accurately from any disaster with minimal data loss, leveraging our backups and infrastructure-as-code.

5. Security Monitoring and Incident Response

Clera has established a comprehensive monitoring framework and incident response plan to rapidly detect, contain, and resolve any security issues. We strive for proactive monitoring to catch issues early, and a practiced response process to handle incidents effectively and comply with breach notification laws. Key elements of our monitoring and IR program:

- **Continuous Security Monitoring:** We maintain 24/7 security monitoring of our production environment. Automated systems and cloud services are in place to detect anomalies in real-time . For example, we use logging and SIEM (Security Information and Event Management) tools to aggregate and analyze logs from AWS CloudTrail, application logs, authentication events, and network flows. Alerts are configured for suspicious patterns such as multiple failed login attempts, unusual data access volumes, or odd network traffic. Our monitoring also covers Cloudflare security events (e.g., spikes in blocked requests). We have a designated on-call engineer for security who will receive automated alerts at any hour if critical thresholds are exceeded. This around-the-clock

vigilance ensures potential threats (like an attempted intrusion or data exfiltration) are identified immediately, not hours or days later .

- **Comprehensive Logging and Auditing:** All critical systems and applications in Clera produce audit logs. We log authentication events, administrative actions, data reads/writes on sensitive resources, and system errors. Logs are timestamped and tamper-evident; they are centralized (using AWS CloudWatch/CloudTrail and our SIEM) for secure storage and analysis. We retain logs for an appropriate period (at least one year for security logs) to support investigations and compliance audits. These logs allow us to trace what happened in detail if an incident occurs, answering the "who, what, when, how" of any security-relevant action. We also perform periodic audit log reviews — manually and with automated checks — to spot any irregularities that automated alerts might miss. Per NIST guidance, having sufficient logging ensures we can adequately investigate and handle incidents .
- **Threat Detection Tools:** In addition to log-based monitoring, we deploy specialized security tools for threat detection. AWS GuardDuty is enabled to intelligently detect malicious or unauthorized behavior in our AWS accounts (such as unusual API calls or known malicious IPs scanning our resources). We also utilize endpoint protection on our servers (and employee laptops) which includes EDR (Endpoint Detection & Response) capabilities to catch malware or intrusion attempts on those systems. Any detection of malware, suspicious process activity, or known attack signatures triggers alerts to the security team. We subscribe to threat intelligence feeds to stay aware of new vulnerabilities or attack campaigns that could target fintech APIs or cloud deployments, and adjust our defenses accordingly. Our goal is a layered detection approach so that whether an attack comes via network, system, or application, some sensor will pick it up.
- **Incident Response Plan:** Clera has a written Incident Response Plan that defines how to handle suspected security incidents. This plan designates an Incident Response Team (including roles such as Incident Lead, Communications Lead, etc.) and outlines the steps of incident handling: Identification, Containment, Eradication, Recovery, and Lessons Learned. When an alert or report indicates a potential incident, we follow a defined process to assess its severity and escalate to the Incident Response Team if confirmed. We have pre-drafted checklists for common scenarios (e.g., server malware infection, data breach exposure, DDoS attack) so responders can act quickly. Containment might involve isolating affected servers or revoking compromised credentials; eradication involves removing malicious code or threat access; recovery might include restoring data from backups and patching vulnerabilities. Throughout the process, we document everything and keep leadership informed.
- **Incident Escalation and Notification:** Incidents are categorized by severity (Low, Medium, High, Critical). For any incident that potentially involves loss of customer data, unauthorized access to PII, or significant service disruption, we immediately escalate to Clera's executive team and simultaneously initiate our communication plan. We are prepared to fulfill any legal notification requirements – for example, GDPR mandates notifying regulators (and users, if high risk) within 72 hours of confirming a personal data breach. Similarly, if an incident involves personal data of Californians, we follow CCPA/CPRA guidance for notifications. Our policy is to be transparent with our

customers and partners: if a data breach occurs, we will inform affected users in a timely manner with details of what happened and what we are doing about it. We will also notify Plaid, Alpaca, or any relevant partner if the incident could impact data we obtained through them, as required under our agreements.

- **Response Training and Drills:** The Incident Response Team members are trained in their roles and responsibilities. We conduct periodic incident response drills (tabletop exercises) to simulate different attack scenarios and practice our response. These drills help us evaluate our readiness and improve the plan by identifying gaps. We also ensure contact information for all team members, including after-hours contacts, is kept up to date (so we can quickly assemble the team if an incident happens at night or on a weekend). By regularly testing our incident response process, we aim to continually refine our ability to handle real incidents. Lessons learned from drills or actual incidents are documented in a post-mortem report, and action items (such as improving a specific control or updating a runbook) are tracked to completion to prevent recurrence.
- **Business Continuity:** Our incident response ties into a broader business continuity and disaster recovery strategy. For example, if a ransomware attack were to occur, our plan calls for a decision on failover to clean systems and restoring from backups. We ensure that our continuity plans (for keeping the service running or getting it back up) align with our incident handling. Critical customer-facing services have redundancy to minimize downtime even during incidents. Our team is empowered to take systems offline if needed to protect data (with communication to users), and to work round-the-clock until normalcy is restored. We also coordinate with third-party security experts or invoke cyber insurance incident response teams if an incident exceeds our internal capacity. The overriding goal is to resolve incidents swiftly, with minimal impact to customers, and to learn from them to strengthen our security posture.

6. Physical Security and Remote Workforce Controls

Clera operates with a largely remote workforce (distributed team members), so our physical security approach focuses on securing endpoints and home office environments, as well as controlling access to data from remote locations. We implement strict policies for device security, network access, and workspace practices to mitigate risks that come with remote work:

- **Secure Endpoints (Laptops & Devices):** Every device used by Clera team members for work must meet our security standards. Laptops/desktops are required to use full-disk encryption to protect data in case of device loss or theft. Strong password or passphrase login is mandated on all devices, and devices must auto-lock after a short inactivity period to prevent unauthorized use. Up-to-date antivirus/anti-malware protection and host firewalls are required on all systems – we centrally ensure updates and patches are applied regularly. We also enable device tracking and remote wipe capability for company-owned laptops. If an employee uses a personal device for any work tasks, that device must adhere to the same policies (or preferably, we encourage using company-managed virtual desktops). Without proper protection, endpoints can become easy points of entry for attackers , so we treat every laptop and phone as a critical part of our security perimeter.

- **VPN and Secure Network Access:** Because our team works from various locations, we require the use of a **Virtual Private Network (VPN)** when accessing any internal company systems or sensitive data from an untrusted network. The VPN enforces an encrypted tunnel for all traffic between the employee and our cloud environment, preventing eavesdropping on public Wi-Fi or home networks. By routing remote endpoint traffic through our corporate VPN, we can also apply internal firewall rules and monitoring to that traffic . For example, access to our staging or production databases is only possible when connected through the VPN and with the proper credentials. We disallow direct connections to cloud consoles or databases from the open internet. In addition, our VPN solution itself requires MFA for login, adding an extra layer of security. In summary, any remote connection to sensitive resources must go through an authenticated, encrypted channel.
- **Device and Software Restrictions:** Clera has a strict policy against installing unauthorized software on work devices. We maintain an approved software list and use endpoint management tools to audit installed applications and browser extensions. High-risk software (e.g., torrent clients or outdated plugins) is forbidden on work machines. We also control administrative rights on company laptops – employees do not run with admin privileges by default, to reduce the impact of malware. External storage (USB drives) usage is restricted and must be encrypted if ever used for transferring work data. All these measures reduce the avenues through which malware or unauthorized access could occur on remote endpoints.
- **Workspace Security Practices:** We expect employees to maintain a secure home or remote office workspace. Team members must ensure that screens cannot be shoulder-surfed by unauthorized persons; using privacy screen filters in public locations is recommended. They must never leave a work laptop unattended in a public space (or in a car, etc.) without it being locked and secured. Sensitive conversations (e.g., discussing architecture or incidents) should be held in private, not loudly in public where they can be overheard. We operate under a mostly paperless workflow for sensitive data – employees should avoid printing documents containing customer PII or credentials. If any physical notes are taken, they should be stored securely and shredded when no longer needed. By instilling good personal security hygiene, we reduce the physical vectors of data compromise.
- **Remote Access Policies:** Access to certain sensitive systems from remote environments is further gated by policy. For instance, production database access might not just require VPN, but also a verified company-issued device. We maintain a tight list of which employees can access what sensitive tools remotely. Administrative interfaces (like our AWS console, CI/CD pipeline, or customer data admin panel) have network restrictions; if possible, we restrict them to corporate VPN IP addresses or specific devices. In some cases, we adopt a zero-trust approach: continuously verifying the user's identity, device security posture, and context for each access. If an employee's machine falls out of compliance (say, missing a patch or antivirus), our endpoint management can block it from connecting to the VPN or corporate apps until the issue is remedied. This ensures only healthy, secure devices are interacting with our sensitive systems.

- **Incident Handling for Devices:** We treat lost or stolen equipment as a security incident. Employees are trained to immediately report if a laptop or phone with company access is lost. Upon such a report, we will remotely lock/wipe the device if possible, and revoke any credentials or active sessions that were on the device (VPN certificates, etc.). We also might force rotation of the user's passwords and tokens. For devices suspected of being compromised by malware, we have procedures to contain and investigate – including possibly requiring the device to be sent back for forensic analysis and providing a replacement. These steps limit damage from physical security incidents involving remote assets.
- **Employee Security Training:** Even though this policy focuses on technical controls, we also require all remote-working staff to complete security awareness training. The training covers topics like phishing avoidance, safe use of home networks (e.g., changing default router passwords), recognizing social engineering attempts, and reporting security issues. We specifically emphasize being cautious with emails or messages that might be phishing, since a dispersed workforce is often targeted that way. Regular security bulletins and reminders are shared to keep security top-of-mind. An informed and vigilant team member is a crucial defense against threats that technology alone might not catch.

7. Third-Party Security and Vendor Management

Clera relies on third-party services such as **Plaid** (for banking connections) and **Alpaca** (for investment account integration), as well as other vendors for cloud hosting (AWS), email, etc. Ensuring our third-party partners maintain high security standards is a critical part of our security program. We manage third-party risk through careful selection, due diligence, and ongoing oversight:

- **Vendor Due Diligence:** Before integrating or partnering with any third-party service, Clera conducts thorough due diligence on the vendor's security posture. We review their security documentation, policies, and compliance certifications. For key partners like Plaid and Alpaca, we verify that they have robust security programs in place (e.g., SOC 2 Type II audits, ISO 27001 certification) and comply with privacy regulations. (Notably, Alpaca publicly adheres to ISO 27001 and undergoes annual SOC 2 Type 2 assessments against all trust criteria , and Plaid likewise is ISO 27001 and SOC 2 certified). We request and review their Service Organization Control (SOC) reports or security whitepapers to understand how they handle data. If any red flags are found (such as weak encryption or past breaches), we either require mitigations or reconsider the partnership. Only vendors meeting our security requirements and industry best practices are approved.
- **Contracts and Security Agreements:** Clera establishes clear agreements with third-party providers that include security and privacy clauses. Our contracts (or Data Processing Agreements) with vendors specify responsibilities for protecting data and require them to notify us promptly in the event of any security breach on their side. For example, our agreement with Plaid will stipulate how user data is handled and that Plaid will maintain its security certifications. We ensure that these vendors commit to

complying with relevant regulations like GDPR/CCPA in handling our users' data. We also include terms about acceptable use of the data (e.g., they cannot use our user data for other purposes without consent). By having these contractual protections, we align the third parties with Clera's own obligations to users.

- **Least Privilege Integrations:** We apply the principle of least privilege to third-party integrations as well. This means we only grant third parties the minimum access or data necessary and vice versa. For example, when using Plaid's API, we utilize scoped access tokens that permit retrieval of the specific account information we need – and users can revoke that access token at any time by unlinking their account . We do not request overly broad data from financial accounts. Similarly, for Alpaca, if we are using API keys for trading on behalf of a user, we limit permissions (if the user only needs read access to their portfolio, we use a read-only key rather than a trading-enabled key). All API keys and secrets for third-party services are stored securely on our side (as noted in Data Handling) to prevent leakage. We isolate third-party credentials so that a compromise of one integration does not automatically grant access to others. Essentially, our integration architecture is designed so that third parties only get what they strictly need and our exposure is limited if a third-party token or service is compromised.
- **Ongoing Vendor Monitoring:** Clera doesn't consider vendor risk a one-time evaluation; we continuously monitor our third parties. We stay informed of any security updates or incident reports from vendors (for instance, if Plaid or Alpaca publishes a security advisory or has an outage or breach, our team evaluates the impact immediately). We maintain contacts with our vendors and subscribe to their technical updates or RSS feeds. On a periodic basis (at least annually), we re-assess critical vendors by checking for updated compliance reports or conducting a review of their performance. We also track any sub-processors that our key vendors use (for example, if Plaid relies on cloud providers or other services, we consider those "fourth-party" risks). If a vendor's security posture degrades or they suffer incidents frequently, we consider mitigating actions (up to and including finding alternative solutions if necessary). All of this is part of our **Third-Party Risk Management** process, which includes keeping an inventory of vendors and the data they have access to, risk-rating them, and ensuring we have appropriate mitigation plans .
- **Compliance and Audits with Partners:** Because we integrate with financial data aggregators, we understand that partners like Plaid may require evidence of our security measures (due diligence). We maintain this comprehensive security policy and supporting procedures to satisfy such requirements. If Plaid or Alpaca conducts a periodic audit or questionnaire of our security (which is common in fintech partnerships), we are prepared to demonstrate our controls (access control, encryption, etc., as documented above). We treat our vendors as extensions of our environment in terms of security – meaning we also extend certain controls to them. For example, we ensure that data we send to third parties is encrypted and free of unnecessary PII. And if a third-party relationship ends, we make sure to revoke their access and require deletion of our data from their systems (as applicable).

- **Incident Response with Third Parties:** Our incident response plan (section 5) includes specific steps for incidents involving third-party services. If a breach occurs that we suspect might involve data held by a vendor, we will coordinate with that vendor's security team, share necessary information under confidentiality, and jointly address the issue. Likewise, if a vendor notifies us of a breach on their side, we will activate our incident plan to assess impact on Clera users and systems, and handle notifications as required. We keep a communication directory of key contacts at Plaid, Alpaca, and other critical suppliers for emergency use. The goal is a swift, coordinated response to limit any damage from third-party incidents.
- **Vendor Security Expectations:** We expect all our third-party service providers to uphold security standards comparable to our own. This includes using encryption, access control, monitoring, and incident management. In fact, both Plaid and Alpaca are known to employ strong encryption (AES-256 for data at rest, TLS for data in transit) and MFA for their internal access . Alpaca operates under a Zero Trust model with strict 2FA for infrastructure access , which aligns with our philosophy. We prefer vendors who are transparent about their security (providing documentation) and who undergo regular independent audits. By selecting reputable, security-forward partners, we reduce overall risk to Clera and its users' data.

Review and Maintenance: This Information Security Policy will be reviewed at least annually and after any significant changes to Clera's systems or regulatory environment. Updates will be made to address new threats, business changes, or compliance requirements. All Clera employees (and contractors) must familiarize themselves with this policy and affirm their understanding. Security is a continually evolving field, and Clera is committed to continuously improving our defenses and practices to protect our users and partners.