CERES

Data Protection and Privacy Policy

www.cerescoin.io

CERES Data Protection & Privacy Policy

Version:	SOP-006 V_1.0
Date of version:	July 4, 2024
Created by:	Mike Carter, Advisor, FTI Consulting; Bobby Lowe, FTI Consulting
Approved by:	Charlie Uchill
Document owner:	Chief Compliance Officer
Classification level:	Proprietary Information
Next review date:	March 31, 2025

Descriptions of the CERES platform, programs, policies, and all other information contained herein are for the sole, exclusive use of CERES owners, employees, and authorized agents/contractors. This document confers no rights to any third party. **CERES reserves the right to update, change, modify, or cancel anything in this document at any time and at the sole discretion of CERES.**

Background

The purpose of this document is to describe the measures undertaken by Compliance, in cooperation with other business functions, to comply with various US data privacy regulations and related guidance. Many of these measures are captured elsewhere in CERES policies, procedures, and controls, but are also referenced here for summarization and to add additional detail for controls related, but not limited to:

1. CFPB- Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation[1]
2. WA State- Consumer financial information privacy under the Gramm-Leach-Bliley Act (GLBA) and Regulation P[2]
3. CA State- California Consumer Privacy Act[3]
4. VA State- Consumer Data Protection Act[4]

[1] https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf
[2] https://apps.leg.wa.gov/WAC/default.aspx?cite=208-690-260
[3] https://oag.ca.gov/privacy/ccpa
[4] https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+SB1392ER+pdf;

5. CO State- Colorado Privacy Act[5]
6. SEC 17 CFR Parts 240, 248, 270, and 275[6]
7. Any other data regulations that CERES may become obligated to either by new legislation or gaining licensure in new jurisdictions[7]

Personal Information

As used herein, "Personal Information" means any information relating to an identified or identifiable natural person (each, a "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, and/or an online identifier or to one or more factors specific to the physical, economic, cultural or social identity of that natural person.

Policy

It is CERES' policy to ensure reasonable steps are taken to maintain controls, oversight, and governance activities related to data privacy and protection as governed by US and various state regulators where CERES is permitted to operate.

1. CERES will appropriately secure customer data.[8]
2. CERES protocols will appropriately address access to data by customers.
3. CERES will limit access by third-parties to uses required to meet regulatory obligations such as (but not limited to) AML/BSA, OFAC, anti-fraud, etc.
4. CERES Terms of Service will appropriately inform and guide data scope and usability, control and consent, and transparency of use.
5. CERES' Customer Support mechanisms will provide appropriate channels for customers to resolve relevant disputes in a timely manner.
6. CERES, in practice, will not use customer data for purposes contrary to consumer financial protection principles.

CERES, by design and intent, adheres to the concepts of:

1. Lawful, fair and transparent processing;
2. Limitation of purpose, data and storage;
3. Data subject rights;
4. Consent; and

---

[5] https://coag.gov/resources/colorado-privacy-act/
[6] www.sec.gov/files/rules/final/2024/34-100155.pdf
[7] CERES does not operate in the EU and is therefore not specifically obligated to GDPR. However, some partners may possess GDPR obligations, and CERES will make a best effort to comply with those obligations when feasible and reasonable.
[8] See CERES various information/cybersecurity policies, risk assessments, and related security tests and assessments for more detail.

5. Protection against personal data breaches.

I. Personal Information We Collect

The USA PATRIOT ACT requires all financial institutions to obtain, verify, and record Personal Information that identifies each person who opens an account. This federal requirement applies to all new users. This Personal Information is used to assist the United States government in the fight against the funding of terrorism and money-laundering activities. When users create a CERES Account, we ask for your name, email address, mobile phone number and other identifying Personal Information. See Appendix A for a full list of information collected and retained.

II. Security of Data

1. See the following relevant CERES policies for various components of data security:
    a. Security Policy
    b. Privacy Policy
    c. Physical Security Policy
    d. Business Continuity Plan
    e. Document Retention Policy
    f. Vendor Management Policy
2. CERES will notify applicable regulatory and law enforcement agencies promptly (within 30 days) upon the discovery of a data breach that has potentially compromised customer PII.[9]

III. Use of Data

1. CERES will use customer data in the manner consistent with:
    a. Requirements to meet regulatory obligations;
    b. Requirements to operate the platform and related business activities in an efficient, safe, secure, user-friendly, and useful manner; and
    c. CERES Terms of Service

2. Marketing

[9] In May 2024, the SEC adopted Rule Amendments to Regulation S-P to enhance protection of customer information: https://www.sec.gov/rules/2023/03/regulation-s-p-privacy-consumer-financial-information-and-safeguarding-customer.CERES' related policies are intended to comply with these rules to "adopt written policies and procedures for incident response programs to address unauthorized access to… customer information, including procedures for providing timely notification to individuals affected by an incident… designed to help affected individuals respond appropriately".

a. CERES complies with the CAN-SPAM Act of 2003[10].
b. Marketing staff will consult with Legal prior to making any changes to the CERES website or application that could affect data collection, use, storage, notification, and/or protection obligations.
c. Marketing or other Operations leadership will provide a mechanism for customers (in required jurisdictions) to opt out of targeted marketing communications.

3. Selling Customer Data
    a. CERES does not sell customer data to third-parties without customer permission.
    b. Marketing or other Operations leadership will consult with Legal prior to engaging in plans to sell[11] or actually selling customer data to a third-party, even if customer consent is obtained.
    c. Marketing or other Operations leadership will provide a mechanism for customers (in required jurisdictions) to opt out of sale of data to third-parties prior to engaging in plans to sell or actually selling customer data to a third-party.

IV. Processing Customer Data Requests

1. Requests for Data Erasure
    a. The "right to be forgotten" does not supersede CERES' obligation to retain certain personal data for the purposes of anti-money laundering and counter-terrorism financing for up to seven years.

    b. For requests that may qualify for personal data erasure past the five-year retention obligation, the effective date of last qualifying event shall include the most recent date of:
        i. Deposit
        ii. Withdrawal
        iii. Limit or market order placed
        iv. Limit or market order canceled
        v. Change of customer CIP information
        vi. SAR or CTR filed
        vii. OFAC report filed (i.e., Blocked Property Report)
        viii. Escheatment filings or disbursements

    c. All data erasure requests will be made via secure Customer Support channels or legal order in order to ensure the security of customer accounts.

---

[10] 16 CFR Part 316; https://www.ecfr.gov/current/title-16/part-316
[11] Defined as the exchange of personal data for monetary consideration.

d. Data erasure requests will be routed through the AML/BSA Officer to ensure:
    i. Customer meets qualifying erasure criteria;
    ii. Customer does not reside in a jurisdiction that requires a longer records retention period (i.e., GDPR, state-specific obligations, etc.)

e. Data erasure requests that are sourced via legal documentation will be routed to Legal in order to assess the validity of the request and respond appropriately.
    i. Legal will work with Customer Support to ensure that requests via legal documentation are sourced from the actual account holder or their approved proxy (i.e., attorney, etc.).

f. Data erasure may not occur for customers that maintain a balance larger than the minimum balance required to withdraw, as there is reasonable belief that a customer will eventually need to withdraw those funds and CERES will need to maintain related transaction and personal information to meet other compliance obligations including, but not limited to, escheatment, law enforcement requests, etc.
g. Data erasure requests will result in one of the following responses (or similar) to the customer via secure communication or written legal response:
    i. "*Unfortunately, we are unable to erase your personal data at this time. CERES is required to maintain customer information for a period of not less than five years from last qualifying event in accordance with the Bank Secrecy Act.*"; or
    ii. "*CERES will process erasure of your personal data as promptly as possible. That data will include your identification documents, name, date of birth, address, nationality, and other financial information provided by the account holder.*"
h. Execution of data requests will be documented and routed through the CTO or their designated proxy.
i. All relevant data will be deleted, with the exception of the communications related to the actual deletion request (i.e., communications or legal documentation).

2. Requests to Retrieve Information
    a. Customers may request either a list of data components that CERES collects and maintains, or the actual data itself.
        i. If a customer requests a list of data components that CERES collects and maintains, Customer Support may provide the list in Appendix A.

b. All data retrieval requests must be made via secure Customer Support channels or legal order in order to ensure the security of customer accounts.
c. Data requests that are sourced via legal documentation will be routed to Legal in order to assess the validity of the request and respond appropriately.
    i. Legal will work with Customer Support to ensure that requests via legal documentation are sourced from the actual account holder or their approved proxy (i.e., attorney, etc.).

d. Limited order histories may be retrieved via self-service by the customer on the CERES website.

e. On request, complete transaction histories will be collected and provided to the customer by Customer Support, including, but not limited to:
    1. Deposits
    2. Withdraws
    3. Placed orders
    4. Completed orders
    5. Cancelled orders
    6. Transfers
    7. Rewards
    8. Dividends
    9. Statements

f. To facilitate other data retrieval, CERES staff will:
    i. Confirm ownership of the account.
    ii. In Admin, generate a Compliance Report for the account.
    iii. Download Compliance report when ready.
    iv. Provide only the data specifically requested by the customer. Do not provide more data than has been requested.
    v. Provide data in a secure manner as prescribed by the controls outlined in Section I of this policy.

g. Data provided to the customer should be limited in scope to the specific data components and timeframe requested to limit risk of data loss or exposure by the customer.

h. Repeated, excessive, or frequent requests by a customer will be routed to the CCO to determine reasonableness of those requests.

Version table

Version	Effective date	Rationale	Updated by	Approved by
1.0	July 4, 2024	New policy	Mike Carter	Charlie Uchill

Appendix A: Listing of Data Components Collected by CERES

Individuals

- First Name
- Middle Name
- Last Name
- Address
- City
- State
- Postal Code
- Country
- Date of Birth
- Tax ID Number
- Nationality
- Email Address
- Phone Number
- IP Addresses Used
- Cookies
- Devices used to access the CERES platform
- Identification Documents (including images uploaded)
- Intended Use of Assets
- Employment Status
- Occupation
- Source of Wealth
- Individual Annual Income
- Total Assets Amount
- Source Of Funds
- Login Activity
- Transaction Activity
- User-Provided Bank Information
- User-Provided Credit/Debit Card Information
- Acceptance of Terms of Service
- Customer Support Communication
- Medical Marijuana cards (if applicable)

Entities

- Individual data listed above, plus…
- Entity legal name
- Employer Identification Number (“EIN”) or any comparable identification number issued by a government

- Full legal name of all account signatories
- Email address of all account signatories
- Mobile phone number of all account signatories
- Proof of legal existence (e.g., state certified articles of incorporation or certificate of formation, unexpired government-issued business license, trust instrument, or other comparable legal documents as applicable)
- Documentation indicating that the signatories are authorized to act on behalf of the legal entity
- Marijuana licenses
- *Other business information required for corporate customers to determine legitimacy and suitability of the business or legal entity

Appendix B: Notices to Users
CERES may deploy the following (or similar) language to notify customers about various components of the CERES' Data Privacy Policy

By visiting, accessing, or using CERES, you consent to the policies and practices of our privacy policy (the "Privacy Policy") so please read them carefully. If any policies or practices described in this Privacy Policy are unacceptable to you, please do not visit, access, or use CERES. Use of the words "we," "us," or "our" in this Privacy Policy refers to CERES Coin LLC. (d/b/a CERES) and any or all of its affiliates.

PERSONAL INFORMATION
As used herein, "Personal Information" means any information relating to an identified or identifiable natural person (each, a "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, or an online identifier or to one or more factors specific to the physical, economic, cultural or social identity of that natural person.

PERSONAL INFORMATION WE COLLECT
The USA PATRIOT ACT requires all financial institutions to obtain, verify, and record Personal Information that identifies each person who opens an account. This federal requirement applies to all new users. This Personal Information is used to assist the United States government in the fight against the funding of terrorism and money-laundering activities. What this means for you: when you create a CERES Account, we ask you for your name, email address, mobile phone number and other identifying Personal Information.

Personal Information we collect may include the following:

Individual Users — Depending on your level of activity, CERES will attempt to collect, verify, and authenticate the following:

- Email address;
- Mobile phone number;
- Full legal name;
- Social Security Number ("SSN") or a comparable government-issued identification number;
- Date of birth;
- Proof of identity (e.g., unexpired driver's license, passport or other government-issued identification);

- Home address (not a mailing address or P.O. Box); and
- Additional Personal Information or documentation at the discretion of our Operations Staff.
- Medical Marijuana cards (if applicable)

Legal Entities — We attempt to collect, verify, and authenticate the following:

- Entity legal name;
- Employer Identification Number ("EIN") or any comparable identification number issued by a government;
- Full legal name of all account signatories;
- Email address of all account signatories;
- Mobile phone number of all account signatories;
- Principal place of business and/or other physical location;
- Proof of legal existence (e.g., state certified articles of incorporation or certificate of formation, unexpired government-issued business license, trust instrument, or other comparable legal documents as applicable); and
- Documentation indicating that the signatories are authorized to act on behalf of the legal entity.
- Marijuana licenses.

Device Information – Information automatically collected about the device used to access the CERES platform (such as, but not limited to, hardware, operating system, browser, etc.).

Location Information – Information automatically collected to determine your location, including your IP address and/or domain name.

Log Information – Information that is generated by your use of CERES that is automatically collected and stored in our server logs. This may include, but is not limited to, device-specific information, location information, system activity and any information related to CERES services you utilize.

Transactional Information – Information that is generated by your activity, including, but not limited to, trading activity, order activity, deposits, withdrawals, and wallet balances.

Correspondence – Information that you provide to us in correspondence, including creating a wallet or wallets, and with respect to ongoing user support.

COOKIES
Some of our web pages may contain "cookies", or data that is sent to your web browser

and stored on your computer. The purpose of these “cookies” is to allow our server to recognize you as a returning visitor, customize our services, content, and advertising; measure promotional effectiveness; help ensure that your account security is not compromised; mitigate risk and prevent fraud; and to promote trust and safety across our sites and services. We may also use trusted third-party services that track this information on our behalf. In the event you do not wish to receive such cookies, you may configure your web browser to not accept cookies or to notify you if a cookie is sent to you. You are free to decline cookies if your web browser permits, but you may not be able to use all the features and functionalities of our website. CERES does not link the information we store in cookies to any personally identifiable information you submit while on our website.

HOW WE USE AND SHARE THE PERSONAL INFORMATION WE COLLECT

The Personal Information we collect, and the practices described above are done in an effort to provide you with the best experience possible, protect you from risks related to improper use and fraud, and help us maintain and improve the CERES platform.

We may share Personal Information with third-party service providers (including those that may be located outside of the United States or your country), who help us operate our platform and systems, and detect fraud and security threats during the normal course of our business. Such third-party service providers are subject to strict confidentiality obligations.

For example, we may use your Personal Information to:

Provide you with our services, including user support for CERES;

- Optimize and enhance our services for all users or for you specifically;
- Conduct anti-fraud and identity verification and authentication checks (you authorize us to share your Personal Information with our third-party service providers, who may also conduct their own searches of publicly available Personal Information about you);
- Monitor the usage of our services, and conduct automated and manual security checks of our services; and
- Create aggregated and anonymized reporting data about our services.

If we decide to modify the purpose for which your Personal Information is collected and used, we will amend this Privacy Policy.

If we propose to sell or buy any business or assets, we may disclose your Personal Information in an anonymized form to the prospective buyer or seller of such business or assets. In the event of a merger, acquisition, or asset sale of CERES, we will give

you notice if, and before, your Personal Information is transferred in a non-anonymized form or becomes subject to a different privacy policy.

CERES may, under certain circumstances and in its sole discretion, disclose your information if we believe that it is reasonable to do so. Such disclosure or transfer is limited to situations where the personal data are required for the purposes of (1) provision of the services, (2) pursuing our legitimate interests, (3) law enforcement purposes, or (4) if you provide your prior explicit consent.

Such reasonable disclosure cases may include, but are not limited to:

- Satisfying any local, state, or Federal laws or regulations;
- Responding to requests, such as discovery, criminal, civil, or administrative process, subpoenas, court orders, or writs from law enforcement or other governmental or legal bodies;
- Bringing legal action against a user who has violated the law or violated our Terms of Use;
- As may be necessary for the operation of CERES;
- Generally cooperating with any lawful investigation about our users; or
- If we suspect any fraudulent activity or have noticed any activity which may violate our Terms of Use or other applicable rules.

DATA SECURITY

Protection of Personal Data

We take the protection and storage of your personal data very seriously and take all reasonable steps to ensure the ongoing confidentiality, integrity, and availability of your personal data. We protect your personal data by using reasonable security safeguards against loss or theft, unauthorized access, disclosure, copying, use, or modification. Your personal data is stored behind secured networks and is accessible by a limited number of persons who have special access rights to such systems and are required to keep the personal data confidential. We implement a variety of security measures, such as encryption and anonymization when users enter, submit, or access their personal data to maintain the safety of their personal data. Please note, however, that no system involving the transmission of information via the Internet, or the electronic storage of data, is completely secure. Consequently, we are not liable for any loss, theft, unauthorized access, disclosure, copying, use, or modification of your personal data that occurs outside our reasonable control.

Breach notification

Should a personal data breach occur; we will inform the relevant authorities without undue delay and immediately take reasonable measures to mitigate the breach. We

will notify you about such a breach via email as soon as possible but no later than within seven business days.

ACCURACY AND RETENTION OF PERSONAL INFORMATION

We take reasonable and practicable steps to ensure that your Personal Information held by us (i) is accurate with regard to the purposes for which it is to be used, and (ii) is not kept longer than is necessary for the fulfillment of the purpose for which it is to be used, which is when your business relationship with us ends, unless the further retention of your Personal Information is otherwise permitted or required by applicable laws and regulations.

ACCESS, CORRECTION, AND DELETION OF PERSONAL INFORMATION

You have the right to ascertain whether we hold your accurate and current Personal Information, to obtain a copy of the Personal Information that you submitted as permitted by law, and to correct any of your data that is inaccurate. You may also request that we inform you of the type of Personal Information we hold with regard to you, subject to restrictions on our providing copies of certain data pursuant to our obligations under the Bank Secrecy Act ("BSA") and Anti-Money Laundering ("AML") regulations and/or data provided to our legal counsel in defense of a claim against us. You may also request that we delete your Personal Information, subject to restrictions under applicable laws and regulations, such as those related to the BSA and AML. For data access, correction, or deletion requests, please contact privacy@CERES.com. When handling a data access, correction, or deletion request, we check the identity of the requesting party to ensure that he or she is the person legally entitled to make such request. While our policy is to respond to such requests free of charge, we reserve the right to charge you a reasonable fee for compliance with your request should your request be repetitive or unduly onerous.

DIRECT MARKETING

Subject to applicable laws and regulations, we may from time to time send direct marketing materials promoting services, products, facilities, or activities to you using information collected from you. We will provide you with an opportunity to opt-out of such communications and will only send them to you if you consent.
We do not sell user Personal Information to third parties for the purpose of marketing.

EU-U.S. PRIVACY SHIELD AND SWISS-U.S. PRIVACY SHIELD

As a global entity, CERES may store, transfer, and otherwise process your personal information in countries outside of the country of your residence, including the United States and possibly other countries.

CERES complies with the *EU-U.S. Privacy Shield Framework and/or the Swiss-U.S. Privacy Shield Frameworks*, as set forth by the U.S. Department of Commerce

regarding the collection, use, and retention of personal information transferred from the *European Union and Switzerland* to the United States. CERES has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

CERES is responsible for the processing of personal information it receives under the Privacy Shield Framework and subsequently transfers to a third party acting as an agent on its behalf. Pursuant to the Privacy Shield Principles, CERES will use personal information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. We take all reasonable steps to ensure that personal information we process is limited to only what is relevant to the purposes for which it was collected and that it is accurate, complete, and up-to-date.

CERES complies with the Privacy Shield Principles for all onward transfers of personal information from the EU and/or Switzerland, including the onward transfer liability provisions. Consequently, before CERES shares your information with any third party that is not also certified under the EU-U.S. Privacy Shield and/or the Swiss-U.S. Privacy Shield Frameworks, CERES will enter into a written agreement that the third party provides at least the same level of privacy safeguard as required under those Frameworks, and assures the same level of protection for the personal information as required under applicable data protection laws.

COMPLAINTS ABOUT HANDLING OF PERSONAL DATA

CERES commits to resolve European and/or Swiss data subjects' complaints about their privacy and our collection, use or disclosure of their personal information in compliance with the EU-U.S. Privacy Shield and/or the Swiss-U.S. Privacy Shield Principles. You have the right to submit a complaint to us about the way in which your personal data have been handled by using the contact details indicated in the "Contact Us" section of this Privacy Policy.

After you submit such a complaint, we will send you an email within five business days confirming that we have received your complaint. Afterwards, we will investigate your complaint and provide you with our response within a reasonable timeframe.

If you are a European and/or Swiss Data Subject with an unresolved complaint or dispute arising under the requirements of the Privacy Shield Frameworks, you may refer your complaint under the Frameworks to an independent dispute resolution mechanism, free of charge to you. Our independent dispute resolution mechanism is

JAMS Mediation, Arbitration and ADR Services ("JAMS"). You may contact JAMS at https://www.jamsadr.com/eu-us-privacy-shield.

We are also subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission with respect to the Framework. Please note that under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel if your complaint is not resolved through the mechanisms describes above.

If you are a resident of the European Union and you are not satisfied with the outcome of your complaint, you have the right to lodge a complaint with your local data protection authority.

CONTACT US

If you are located in the EU or Switzerland and have questions or concerns regarding the processing of your Personal Information, you may contact us at: privacy@CERES.com or write us at:

CERES Coin LLC.
332 South Michigan Ave, Suit 121-F7
Chicago, IL 60604
USA