LUNARBITS222.COM

Information Security and Data Protection Procedures

Non-Custodial Model: Recommend Third-Party Wallets Only

Effective Date	November 20, 2026
Version	1.0
Applies To	All personnel, contractors, and systems associated with lunarbits222.com and related Lunarbits activities

1. Purpose and Scope

These procedures establish administrative, technical, and physical safeguards for the protection of customer, user, and investor information processed or stored in connection with lunarbits222.com.

Lunarbits222 does not custody customer private keys, digital assets, tokens, or funds. The platform and associated entities only recommend third-party wallet providers (e.g., Unisat.io, Xverse.io, or other user-controlled wallets). Users maintain exclusive control of their private keys and assets at all times. Lunarbits has no ability to access, move, freeze, or recover user assets.

These procedures apply to:

- Website forms, applications, and communications
- Any investor or user data collected (including for Reg D equity token offerings)
- Internal systems, email, cloud storage, and third-party tools
- All personnel with access to such information

2. Non-Custodial Position

- Lunarbits222.com and related entities do not hold, control, or have access to customer private keys or digital assets.
- All wallet recommendations are informational only. Users are solely responsible for securing their own wallets and seed phrases.
- No custody services are offered. Any statements or marketing must clearly reflect this non-custodial model.
- In the event of user inquiries about lost keys or compromised wallets, staff must direct users to their wallet provider and confirm Lunarbits cannot assist with recovery.

3. Regulatory Alignment

Procedures are designed to support compliance with applicable requirements, including:

- SEC Regulation S-P (safeguards and incident response for customer information), as amended
- Regulation S-ID (identity theft red flags), where covered accounts exist
- General privacy and data protection expectations
- Alignment with ISO/IEC 27001 principles and NIST Cybersecurity Framework best practices (not a formal certification mandate)

If Lunarbits or affiliated entities are or become a covered institution (e.g., through securities activities), these procedures form part of the required written safeguards program.

4. Roles and Responsibilities

- **Designated Security/Compliance Lead:** Responsible for implementing and maintaining these procedures, conducting periodic reviews, and coordinating incident response.
- **All Personnel:** Must follow these procedures, complete required training, and immediately report suspected incidents or unauthorized access.
- **Management:** Provides resources and oversight. Reviews the program at least annually.

5. Data Classification and Handling

Customer/User Information includes any nonpublic personal information, contact details, application data, investor qualification information, wallet addresses submitted by users, or similar data.

Requirements:

- Collect only data necessary for the stated purpose.
- Store data only in approved, access-controlled systems.
- Encrypt sensitive data in transit (TLS 1.2+) and at rest where feasible.
- Limit access on a need-to-know basis.
- Retain data only as long as necessary for business, legal, or regulatory purposes, then securely dispose of it.
- Do not request or store private keys, seed phrases, or recovery phrases under any circumstances.

6. Access Control Procedures

- Unique user accounts with strong passwords (or equivalent) and multi-factor authentication (MFA) for all systems that can access customer information.
- Principle of least privilege: Grant only the minimum access required.
- Promptly remove access upon termination or role change.
- Periodic access reviews (at least annually).
- No shared accounts for systems containing customer data.

7. Incident Response Procedures

An incident includes unauthorized access to or use of customer information, or a reasonable likelihood thereof.

Steps:

1. **Detect and Report:** Any personnel who suspects an incident must immediately notify the Security/Compliance Lead.
2. **Assess:** Determine the nature, scope, and systems/data involved. Document findings.
3. **Contain and Recover:** Take appropriate steps to stop unauthorized access, mitigate impact, and restore normal operations.
4. **Notify (as required):**
    - Affected individuals if sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization (as soon as practicable, generally no later than 30 days after awareness, consistent with Regulation S-P).
    - Service providers must be contractually required to notify Lunarbits within 72 hours of becoming aware of a breach involving a customer information system they maintain.

5. **Document:** Maintain records of the incident, response actions, and notifications for at least three years.
6. **Post-Incident Review:** Identify lessons learned and update procedures as needed.

8. Vendor and Third-Party Management

- Maintain a list of service providers that receive, process, or store customer information.
- Perform due diligence before engagement and periodically thereafter.
- Contracts must require providers to protect customer information and notify Lunarbits of relevant security incidents within 72 hours.
- Wallet providers and exchanges recommended to users are third parties; Lunarbits does not control their security and must not imply otherwise.

9. Technical and Operational Controls

- Use of secure, reputable hosting and email providers.
- Regular software updates and patching.
- Logging and monitoring of access to systems containing customer data.
- Data loss prevention practices (e.g., monitoring for unauthorized outbound transmission of sensitive data).
- Secure development and change management for the website where applicable.
- Regular backups of critical systems with tested recovery.

10. Training and Awareness

- Personnel with access to customer information must receive initial and periodic training on these procedures, phishing awareness, and incident reporting.
- Training records are maintained.

11. Review and Updates

- These procedures are reviewed at least annually, or upon significant changes in business, technology, or regulations.
- Updates are approved by management and communicated to relevant personnel.

12. Contact

Questions or incident reports: Direct to the designated Security/Compliance Lead
lunarbitsdao@gmail.com

Disclaimer

These procedures reflect the stated non-custodial model (recommend third-party wallets only; no custody of private keys or digital assets) while addressing the protection of any customer or user data that is collected or processed.