ACCREDEFI INFORMATION SECURITY POLICY & OPERATIONAL PROGRAM OVERVIEW (V1.0)

1. Policy Statement and Scope

AccreDeFi establishes this Information Security Policy (ISP) to ensure the confidentiality, integrity, and availability of all critical assets, data processed, and smart contract logic deployed across the TON and XDC networks. Our mandate is to operate as an institutional enforcement protocol that facilitates secure asset tokenization exclusively for licensed asset managers. The scope of this policy covers all deployed software, infrastructure-as-code (IaC), and administrative functions within the current Minimum Viable Product (MVP) operational footprint.

2. Governance, Risk Management, and Compliance (GRC)

The organization maintains a formalized, operational information security program guided by this documented policy. Risk management is fundamentally driven by Data Minimization and Compliance by Enforcement.
To mitigate third-party risk, all external compliance data is validated by a secure Oracle Bridge using cryptographic signatures (JWT/JWK standard). Our core risk mitigation strategy centers on the Cryptographic Identity Anchor, which is a unique, unforgeable hash linked to the user's verified identity. This anchor is used to enforce all compliance checks.

- Integrity Control: We operate a Wallet Recovery Protocol implemented within the Reputation Engine to actively penalize score migration, preventing unauthorized attempts to evade the historical compliance record.
- Data Handling: We adhere to the principle of least privilege. We minimize sensitive data retention; the system relies on external providers (like Plaid) for initial PII and only receives and commits the final, cryptographically validated compliance status to the on-chain Oracle.

3. Operational and Technical Controls

AccreDeFi actively enforces security controls across its infrastructure and personnel environments.

Endpoint Security and Visibility

We maintain continuous and comprehensive visibility into all network assets. The organization utilizes automated tools and Infrastructure-as-Code (IaC) via Terraform and Docker to discover and

maintain continuous visibility into all network endpoints, including servers, virtual machines, and databases. We actively perform vulnerability scans against all production assets and address identified vulnerabilities using a strict, defined Service Level Agreement (SLA) for patching. Endpoint security agents are deployed across all production assets to protect against malicious code, viruses, and malware.

Access Control and Authentication

Security controls are uniformly applied across all critical access points. We have deployed strong factors of authentication (MFA) for all critical assets, including cloud consoles, code repositories, and secrets management vaults. Furthermore, access to all resources is managed via explicitly defined, documented processes for requesting, granting, reviewing, approving, and revoking access.

Device Policy

AccreDeFi maintains a policy against the use of personal devices for carrying out job responsibilities. We do not operate a Bring Your Own Device (BYOD) policy. All access to critical production assets and data is conducted using company-provided and managed devices, simplifying the security posture and ensuring a consistent level of endpoint protection.

4. Operational Commitment

This documented policy is fully integrated into the development lifecycle and operations of the AccreDeFi MVP. Compliance with these controls ensures that the protocol maintains the highest standards of integrity required to serve licensed asset managers and financial institutions, providing a secure and auditable foundation for compliant tokenization.