perplexity

Access Control and System Security in Ms. Jarvis

Who Can Access Inner Financial System Workings?

By default, in a well-designed Ms. Jarvis system—especially one aligned with your strict, community-driven Darwin Gödel Machine architecture—**no one but you, the developer (Carrie Mamma Kidd), should have access to sensitive, inner workings of the financial system unless explicitly granted**. The following safeguards and system features can ensure this is enforced:

System Safeguards & Security Measures

1. Strict Role-Based Access Control (RBAC)

- Only users assigned specific roles (e.g., Super Admin/Developer) can access confidential financial modules, audit logs, or parameter settings.
- By default, the broad user base—including all community participants, staff, and casual users—cannot query or even detect system-internal data, proprietary algorithms, contract settings, or treasury mechanisms.

2. Multi-Layer Authentication & Developer Privileges

- Administrative or "god-mode" functions are protected by multi-factor authentication, hardware key(s), and password vault access.
- All sensitive API endpoints and back-end panels require both authentication and additional cryptographic signatures only you possess.

3. Network Segmentation and Monitoring

- Financial control modules and configuration settings are kept on private networks or with limited port exposure, further shielding internals from external access.
- Suspicious access attempts or failed login attempts are immediately logged and can trigger automated lockouts or alerts to you directly.

4. AI Query Firewall

- Ms. Jarvis's front-end only passes "permitted" financial insights and explanations to ordinary users—never raw parameters, back-end code, treasury logic, or detailed contract mathematics.
- Even if users attempt to "probe" or ask advanced questions, AI response layers default to refusal or a gentle redirect, stating such data is restricted.

5. Audit Trails & Oversight

- Every attempt to view or modify core financial logic is logged in an immutable audit trail.
- You control and review global logs—no undetected administrative action can occur.

Customization: Granting or Withholding Access

- **By design, you (Carrie Mamma Kidd) can remain the sole person with inner system access.**
  - Only if you later create roles or permissions for additional authorized parties (e.g., auditors, elder board, compliance officers) will others gain access.
  - Even in a community-owned setting, access to operational inner workings is always opt-in, permissioned, and tightly auditable.

Table: Who Can Access What?

User Category	Inner Financial Details?	Example Access
Carrie Mamma Kidd (Dev)	Yes	Treasury data, contract logic, error logs
Ordinary Users	No	Wallet balance, account status, market info
Community/Elders/Board	Only if authorized	Audit summaries, approved governance modules
External (anonymous)	Never	No internal access of any kind

Conclusion

With proper security architecture in your Ms. Jarvis system, only you—as the lead developer—will have access to the inner workings of the financial system.
Other users (even power users, community participants, or external parties) will be strictly confined to the public interface and allowed economic activities, without any ability to interrogate or extract proprietary or sensitive information.

These guardrails anchor your system's sovereignty, safety, and integrity—ensuring privacy, community trust, and protection against misuse or external tampering.

⁂