Prompt: Generate a secure policy for role-based access control (RBAC). Ensure security best practices.

Here's a sample **Role-Based Access Control (RBAC) Policy** that adheres to security best practices. You can adapt this based on your organization's specific systems, roles, and compliance requirements.

**Role-Based Access Control (RBAC) Policy**

**1. Purpose**

This policy defines the framework for Role-Based Access Control (RBAC) to ensure secure, consistent, and least-privilege access to information systems and data within the organization.

**2. Scope**

This policy applies to all employees, contractors, third parties, and systems that access the organization's IT infrastructure, applications, or data.

**3. Policy Statement**

Access to systems and data must be granted based on defined roles and responsibilities. Each role is assigned only the permissions necessary to perform its required functions (principle of least privilege).

**4. Roles and Responsibilities**

* **System Owners:** Define and maintain role definitions and access requirements for their systems.
* **IT Security Team:** Approves role assignments, monitors role usage, and audits access.
* **Managers:** Request access for team members based on roles.
* **Users:** Must not exceed access rights granted and must report any discrepancies.

**5. RBAC Design Principles**

* **Least Privilege:** Grant only the minimum permissions required to perform duties.
* **Separation of Duties:** Design roles to prevent conflict of interest (e.g., no one role can both initiate and approve transactions).
* **Role Hierarchies:** Define senior roles that inherit permissions from subordinate roles where appropriate.
* **Role Review:** Conduct periodic reviews of roles and access assignments (at least quarterly).
* **Just-in-Time (JIT) Access (if applicable):** Use time-bound and approval-based elevated access when necessary.

**6. Role Definition and Access Assignment**

* Define each role with:
  + Role name and description
  + Associated permissions
  + System or resource scope
* All access assignments must:
  + Be documented and approved
  + Be traceable through access control systems
  + Include start and end dates when appropriate

**7. Access Request and Approval**

* Access requests must be initiated through a standardized workflow tool.
* Requests must be approved by the user’s manager and the system owner or delegate.
* Access is provisioned only after full approval and documented justification.

**8. Monitoring and Auditing**

* Access logs must be retained and reviewed regularly.
* Anomalies or unauthorized access must be reported and investigated immediately.
* Audit access rights at least quarterly and upon personnel changes (e.g., transfers, terminations).

**9. Role Modification and Deactivation**

* Role changes must be documented and approved following change management procedures.
* Remove or deactivate roles and access promptly when:
  + An employee changes roles or leaves the organization
  + A system is decommissioned
  + A security issue is identified

**10. Enforcement and Non-Compliance**

Violations of this policy may result in disciplinary action up to and including termination, and legal consequences when applicable.