Prompt: Generate a policy for role-based access control (RBAC).

Here is a comprehensive **Role-Based Access Control (RBAC) Policy** that you can adapt for your organization:

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

**Policy Number**: [Insert Number]  
**Effective Date**: [Insert Date]  
**Last Reviewed**: [Insert Date]  
**Next Review Date**: [Insert Date]  
**Approved By**: [Insert Authority]

**1. Purpose**

The purpose of this policy is to define and enforce Role-Based Access Control (RBAC) to ensure that access to systems and data is granted based on job responsibilities and the principle of least privilege. RBAC reduces security risks and supports regulatory compliance.

**2. Scope**

This policy applies to all users—including employees, contractors, vendors, and temporary staff—who access the organization's information systems and data.

**3. Policy Statement**

* Access to information systems will be managed based on roles rather than individual user accounts.
* Each role will have predefined permissions aligned with business functions and responsibilities.
* Users will be assigned to one or more roles based on job duties, and will inherit associated access rights.
* All access rights must be approved, documented, and reviewed periodically.
* Roles and associated permissions must be reviewed at least quarterly or upon major organizational changes.

**4. Roles and Responsibilities**

| **Role** | **Responsibility** |
| --- | --- |
| **IT Security Team** | Define roles, enforce policy, monitor access, and conduct regular audits. |
| **Managers** | Request and approve role assignments based on job responsibilities. |
| **HR Department** | Notify IT of new hires, terminations, or changes in job functions. |
| **System Owners** | Define resource-specific access needs and role requirements. |
| **Users** | Follow access guidelines and report unauthorized access or breaches. |

**5. Role Management Process**

* **Role Definition**: Roles must be clearly defined, including the systems and data they can access.
* **Access Assignment**: Access requests must follow the access request workflow and be approved by the user’s manager and IT.
* **Review and Revocation**: Roles and permissions must be reviewed quarterly. Access for terminated or transferred users must be removed immediately.

**6. Enforcement**

* Violations of this policy may result in disciplinary action, including revocation of access, reporting to authorities, or termination.
* System logs and monitoring tools will be used to detect unauthorized access attempts.

**7. Exceptions**

Any exception to this policy must be documented, justified, and approved by the Information Security Officer.

**8. Review and Updates**

This policy must be reviewed annually or when significant changes to systems or business processes occur.