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

**ROLE-BASED ACCESS CONTROL (RBAC) POLICY**

**Version:** 1.0  
**Effective Date:** [Date]  
**Review Cycle:** Annual

**1. Purpose**

To minimize security risks by ensuring users access only systems, applications, and data required for their job functions, adhering to the **Principle of Least Privilege (PoLP)**.

**2. Scope**

Applies to all:

* Employees, contractors, interns, and third parties
* On-premises systems, cloud services, databases, and networks
* Production, development, and testing environments

**3. Core Principles**

* **Least Privilege:** Users receive only permissions essential to their role.
* **Separation of Duties (SoD):** Critical actions require multiple roles (e.g., requester + approver).
* **Role Hierarchy:** Senior roles inherit permissions of junior roles (e.g., Manager > Analyst).
* **Zero Standing Privileges:** Elevated access (e.g., admin) is granted temporarily only.

**4. Definitions**

| **Term** | **Definition** |
| --- | --- |
| **Role** | Collection of permissions tied to a job function (e.g., "HR\_Recruiter"). |
| **Permission** | Authorization to perform an action (e.g., read:payroll\_data). |
| **User** | Human or system account accessing resources. |
| **Access Review** | Periodic audit of user-role assignments. |

**5. Roles & Responsibilities**

| **Party** | **Responsibilities** |
| --- | --- |
| **IT Security** | Create/update roles; conduct access reviews; audit compliance. |
| **HR** | Notify IT of hires/role changes/terminations within 24 hours. |
| **Department Managers** | Request role assignments; validate quarterly access reviews. |
| **Users** | Report suspicious access; never share credentials or circumvent controls. |

**6. Access Management Procedures**

**6.1 Role Creation**

* Roles require documented business justification and approval by IT Security + relevant department head.
* Roles must align with SoD (e.g., "Payment\_Approver" and "Payment\_Processor" are separate).

**6.2 User Provisioning**

* Access granted **only after** HR onboarding confirmation.
* Default roles assigned per job title (e.g., "Sales\_Representative").

**6.3 Access Modification**

* Role changes require manager approval via ticketing system.
* Immediate revocation upon termination (automated via HR-IT integration).

**6.4 Temporary Access**

* Max duration: **72 hours** (e.g., for system maintenance).
* Requires CISO/designee approval and logging of justification.

**7. Compliance & Enforcement**

* **Access Reviews:** Quarterly for privileged roles; annually for standard roles.
* **Audits:** Bi-annual RBAC policy compliance audits.
* **Violations:** Unauthorized access may result in suspension, termination, or legal action.

**8. Prohibited Activities**

❌ Sharing user accounts  
❌ Bypassing approval workflows for role assignments  
❌ Permanent use of privileged roles (e.g., global admin)

**9. Policy Maintenance**

* Reviewed annually by IT Security and Legal.
* Updated after security incidents, infrastructure changes, or regulatory shifts (e.g., GDPR, HIPAA).

**Approved By:**  
[Name], Chief Information Security Officer  
[Name], Chief Human Resources Officer  
**Date:** [Date]

**Implementation Guidance:**

* Use automated tools (e.g., Azure RBAC, AWS IAM) for role assignments.
* Integrate HRIS (e.g., Workday) with IAM systems for real-time provisioning/deprovisioning.
* Maintain a **Role-Permission Matrix** (see *Appendix A*).

*(Attach Appendix A: Sample Role-Permission Matrix Template)*