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

**Role-Based Access Control (RBAC) Policy**  
**Version:** 2.0  
**Effective Date:** [Insert Date]  
**Last Reviewed:** [Insert Date]  
**Approved By:** [Name/Title]

**1. Purpose**

This policy establishes a standardized framework for managing access to organizational resources through Role-Based Access Control (RBAC). It ensures alignment with security best practices, including the principle of least privilege (PoLP), segregation of duties (SoD), and compliance with regulatory standards (e.g., NIST, ISO 27001, GDPR).

**2. Scope**

This policy applies to:

* All employees, contractors, vendors, and third parties.
* All systems, applications, databases, networks, and data (on-premises, cloud, and hybrid environments).

**3. Roles and Responsibilities**

| **Role** | **Responsibilities** |
| --- | --- |
| **IT Security Team** | - Define, maintain, and audit RBAC roles. - Enforce SoD and PoLP. - Manage access revocation. |
| **Department Managers** | - Validate role-based access needs. - Approve access requests and changes. |
| **Data Owners** | - Classify data sensitivity. - Approve access to high-risk systems/data. |
| **Employees/Contractors** | - Use access only for authorized tasks. - Report suspicious activity. |
| **Auditors** | - Conduct independent reviews of RBAC compliance. |

**4. RBAC Implementation Guidelines**

**4.1 Role Definition**

* **Role Creation**: Roles must align with job functions (e.g., "HR Manager," "DevOps Engineer").
* **Least Privilege**: Assign the minimum permissions required to perform duties.
* **Conflicting Roles**: Prohibit combining high-risk roles (e.g., "Account Approver" and "Payment Processor").

**4.2 Access Assignment**

* **Approval Workflow**: Access requires approval from the requester’s manager, Data Owner (if sensitive), and IT Security.
* **Temporary Access**: Granted only with justification and an expiration date (max 30 days).
* **Default Access**: New users receive "deny by default" until explicitly approved.

**4.3 Access Reviews**

* **Frequency**:
  + **Standard Roles**: Quarterly reviews.
  + **High-Risk Roles** (e.g., admin, finance): Monthly or bi-annual reviews.
* **Triggers**: Immediate review upon role changes, termination, or security incidents.

**4.4 Authentication & Authorization**

* **MFA**: Required for all privileged roles (e.g., system administrators).
* **Session Management**:
  + Inactivity timeout: 15 minutes for standard users; 5 minutes for privileged roles.
  + Encrypted sessions for remote access.
* **Password Policies**: Enforce complexity, 90-day rotation, and no reuse.

**4.5 Monitoring & Auditing**

* **Logging**: Record all access requests, approvals, and changes.
* **Alerts**: Trigger alerts for unauthorized access attempts or privilege escalation.
* **Audit Trails**: Retain logs for [X] years (align with regulatory requirements).

**5. Access Request Process**

1. **Request**: Submit via secure IT portal with business justification.
2. **Approval**: Multi-tier approval (manager, Data Owner, IT Security).
3. **Provisioning**: Automated role-based access assignment via IAM tools.
4. **Documentation**: Update access control lists (ACLs) and notify the user.
5. **Emergency Access**: Requires CISO approval and post-hoc review.

**6. Violations & Enforcement**

* **Violations Include**:
  + Sharing credentials.
  + Unauthorized privilege escalation.
  + Bypassing approval workflows.
* **Consequences**:
  + First offense: Mandatory training and access suspension.
  + Repeat offenses: Disciplinary action up to termination.
* **Incident Response**: Investigate breaches stemming from RBAC failures and update controls.

**7. Compliance & Training**

* **Regulatory Alignment**: Adhere to [GDPR/HIPAA/PCI-DSS] as applicable.
* **Training**: Annual RBAC and security awareness training for all personnel.
* **Third Parties**: Contractually mandate RBAC compliance and limit access scope.

**8. Policy Review & Updates**

* Reviewed annually or after significant changes (e.g., mergers, new regulations).
* Updates require approval from [CISO/IT Governance Board].

**Approval Signature:**  
[Name]  
[Title]  
[Date]