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

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

Effective Date: [Insert Date]

Last Reviewed: [Insert Date]

Policy Owner: [Insert Department/Role, e.g., IT Department, Chief Information Security Officer]

1. Purpose

This Role-Based Access Control (RBAC) Policy defines the requirements and procedures for managing access to [Organization Name]'s information systems and resources. The primary goal of this policy is to ensure that users have appropriate access to the information and resources necessary to perform their job duties, while protecting sensitive information from unauthorized access, modification, disclosure, or destruction. This policy supports the principle of least privilege, granting only the minimum necessary permissions required for a user's assigned role.

2. Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other third parties (collectively referred to as "Users") who require access to [Organization Name]'s information systems, networks, applications, and data (collectively referred to as "Systems"). This includes, but is not limited to:

* All company-owned or leased hardware and software.
* All data created, stored, or transmitted on [Organization Name]'s Systems.
* All cloud-based services and platforms utilized by [Organization Name].

3. Policy Statements

3.1. Principle of Least Privilege

All access rights shall be granted based on the principle of least privilege. Users will only be granted the minimum level of access and permissions necessary to perform their explicitly assigned job responsibilities.

3.2. Role-Based Access

* Access to Systems shall be managed through predefined roles.
* Roles shall be defined based on job functions, responsibilities, and business requirements, rather than individual users.
* Permissions to access specific resources and perform actions shall be assigned to roles, not directly to individual users, wherever technically feasible.
* Users shall be assigned to one or more roles based on their job responsibilities.

3.3. Role Definition and Management

* Role Creation: New roles shall be formally requested, documented, and approved by the designated authority (e.g., IT Department, Data Owner, Department Manager) before creation. The request must include a clear description of the role's purpose, responsibilities, and required permissions.
* Role Modification: Any changes to existing roles, including modifications to assigned permissions, must follow a formal change management process and be approved by the designated authority.
* Role Decommissioning: Roles that are no longer required shall be formally decommissioned after appropriate review and approval.
* Role Documentation: A central inventory of all defined roles and their associated permissions shall be maintained and regularly reviewed. This documentation should be accessible to relevant stakeholders.

3.4. User Access Management

* Onboarding: New users shall be assigned appropriate roles based on their job function upon commencement of their employment or engagement. Access shall be granted only after proper authorization.
* Role Changes: When a user changes job functions within the organization, their assigned roles and access permissions shall be reviewed and updated in a timely manner to reflect their new responsibilities. Previous, unnecessary access must be revoked.
* Offboarding: Upon termination of employment or engagement, all access rights and role assignments for the user shall be revoked in a timely manner.
* Temporary Access: Requests for temporary access or elevation of privileges must be justified, documented, approved by the designated authority, and granted for a limited duration. Such access shall be monitored and revoked automatically upon expiration.

3.5. Access Review and Recertification

* Regular reviews of user access and role assignments shall be conducted to ensure appropriateness and compliance with this policy.
* Department Managers or Data Owners are responsible for periodically reviewing the access rights of users within their areas of responsibility.
* The frequency of access reviews shall be determined by the sensitivity of the Systems and data, but shall occur at least [annually/bi-annually/quarterly].
* Any discrepancies or inappropriate access identified during reviews must be promptly remediated.
* Results of access reviews shall be documented and maintained.

3.6. Segregation of Duties

* RBAC implementation shall support the principle of Segregation of Duties (SoD) where appropriate to prevent a single user from having conflicting permissions or excessive control that could lead to fraud, errors, or misuse of Systems.
* Roles and permissions shall be designed to ensure that critical tasks require more than one individual to complete.
* Potential SoD conflicts shall be identified and mitigated through role design or compensating controls.

3.7. Privileged Access Management

* Access to privileged accounts (e.g., administrator, root) shall be strictly controlled and limited to authorized personnel whose job functions specifically require such access.
* The use of privileged accounts shall be logged and monitored.
* Shared privileged accounts should be avoided. If unavoidable, mechanisms for individual accountability (e.g., password vaulting with individual check-out) must be implemented.
* Multi-Factor Authentication (MFA) shall be required for all privileged access.

3.8. Logging and Monitoring

* System and application logs related to access attempts, successful logins, and security-relevant events shall be enabled, collected, and regularly reviewed.
* Monitoring shall be in place to detect unauthorized access attempts, policy violations, and anomalous activity.

4. Responsibilities

* Policy Owner (e.g., IT Department, CISO):
  + Maintain and update this RBAC policy.
  + Oversee the implementation and enforcement of this policy.
  + Provide guidance and support for RBAC implementation.
* IT Department / System Administrators:
  + Implement and maintain the technical infrastructure for RBAC.
  + Create, modify, and decommission roles and manage user role assignments as per approved requests.
  + Ensure appropriate logging and monitoring mechanisms are in place.
  + Conduct regular technical audits of RBAC configurations.
* Department Managers / Data Owners:
  + Define appropriate roles and access requirements for their respective departments or data domains.
  + Request and approve access for users within their areas of responsibility.
  + Conduct regular access reviews and recertification for their users and resources.
  + Ensure compliance with this policy within their teams.
* Users:
  + Understand and adhere to this RBAC policy.
  + Use access rights only for authorized business purposes.
  + Protect their access credentials and report any suspected compromise immediately.
  + Request changes to their access rights through appropriate channels if their job responsibilities change.
* Internal Audit:
  + Periodically audit compliance with this RBAC policy and related procedures.

5. Policy Enforcement

* Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract,1 in accordance with [Organization Name]'s disciplinary policies and applicable laws.
* Suspected violations of this policy should be reported immediately to [Insert Reporting Channel, e.g., IT Helpdesk, Security Team, Manager].

6. Policy Exceptions

* Any exceptions to this policy must be documented, justified, approved by the Policy Owner (or a designated authority), and reviewed periodically.
* Approved exceptions must include compensating controls to mitigate associated risks.

7. Policy Review and Updates

* This policy shall be reviewed at least annually, or as needed due to significant changes in business operations, technology, or regulatory requirements.
* Updates to this policy shall be communicated to all relevant Users.

8. Definitions

* Role: A collection of permissions that define the level of access a user or group of users has to specific resources or functionalities.
* Permission: The authorization to perform a specific action on a specific resource (e.g., read, write, delete, execute).
* Principle of Least Privilege: Granting only the minimum necessary access rights required for a user to perform their job duties.
* Segregation of Duties (SoD): A control mechanism designed to prevent error and fraud by ensuring that no single individual has control over all aspects of a critical transaction or process.
* Privileged Access: Elevated access rights typically granted to system administrators or other IT personnel allowing them to manage and configure systems.
* Multi-Factor Authentication (MFA): A security system that requires more than one method of authentication from independent categories of2 credentials to verify the user's identity.3

9. Related Documents

* [List any related policies, standards, or procedures, e.g., Information Security Policy, Data Classification Policy, Acceptable Use Policy, Change Management Policy, Password Policy]

Approval:

[Name and Title of Approving Authority]

Date