**🛡️ Access Control Policy**

**Document Title:** Access Control Policy  
**Version:** 1.3  
**Owner:** IT Security Team  
**Effective Date:** January 5, 2025  
**Review Cycle:** Annual

**1. Purpose**

The purpose of this policy is to ensure only authorized users have access to systems, applications, and data based on job responsibilities.

**2. Scope**

This policy applies to all employees, contractors, and third-party users accessing the organization’s systems within the cardholder data environment (CDE).

**3. Access Provisioning (7.2.1)**

* Access to system components is granted based on defined roles and job responsibilities.
* Access is granted based on job requirements, but some users are granted broader access to ensure operational efficiency, without a detailed review of the specific privileges needed for each role
* Access assignments are reviewed to ensure alignment with role-based access definitions.

**4. Access Reviews (7.2.4)**

* Access reviews are conducted annually.
* User accounts and access remain appropriate based on job function.
* Managers are responsible addressing any inappropriate access and for certifying user access within their departments.

**5. Account Deactivation (8.2.5)**

* When an employee leaves the company, their access should be removed as soon as possible.
* Termination lists are reviewed weekly by IT.

**6. Remote Access (8.4.3)**

* Multi-factor authentication (MFA) is required for all remote access that could potentially impact or access sensitive data outside the organization's internal network.
* Remote access is facilitated through a secure VPN connection that enforces MFA for all users.
* All remote access events are logged for auditing purposes, with investigations triggered for any suspicious or unauthorized access attempts.

**✅ Embedded Issues Summary:**

| **Section** | **Issue** | **PCI DSS Requirement** | **Suggested Improvement** |
| --- | --- | --- | --- |
| 3 | Some users are granted broad without a detailed review of specific privileges needed. | 7.2.1 | Implement access based on the principle of least privilege. Restrict user access to only what is necessary for their job functions. |
| 4 | * Access reviews are conducted annually. | 7.2.4 | At least once every six months |
| 5 | * When an employee leaves the company, their access should be removed as soon as possible. | 8.2.5 | Access for terminated users is immediately revoked. |
|  |  |  |  |
|  |  |  |  |

**🔍 Instructions:**

1. Read the provided partial Access Control Policy carefully.
2. Use the table above to record any **gaps**.
3. Map your findings to relevant **PCI DSS 4.0.1 requirements**.

**💡 Reflection Questions (Optional)**

1. How would failing to fix one of these gaps impact audit readiness?
2. Imagine you're conducting an assessment of an organization that allows remote access to its network from outside its internal environment. The organization uses a VPN for this access, but you find that multi-factor authentication (MFA) is not implemented. How would you address this gap in the assessment? What steps would you recommend to bring the organization into compliance with industry standards like PCI DSS?