Access Control Policy and Procedures

1. Purpose

The purpose of this Access Control Policy and Procedure document is to ensure that access to user data is strictly controlled and aligned with DocuPanda's commitment to maintaining data security, integrity, and confidentiality. This document outlines policies and procedures for managing, monitoring, and enforcing access controls.

---

2. Scope

This policy applies to all DocuPanda employees, contractors, and users, covering all systems, platforms, and data managed by DocuPanda, including but not limited to:

- **AWS and Azure Storage Buckets**: Where user-uploaded documents are stored.
- **DocumentDB**: Where insights generated from user documents are stored.
- **Privileged Systems and APIs**: Used for backend operations.

---

3. Access Control Policy

3.1 Employee Access

1. **General Employees**
    - Do not have access to any user data.
    - Access is restricted to fake data (publicly available documents or internal non-user-related documents).
2. **Developers**
    - Access to data is limited to development environments using fake data only.
    - No direct access to production environments or user data.
3. **Admins (Cofounders)**
    - The only two employees (cofounders) with access to the privileged API key.
    - Access to user data is limited to legitimate business purposes, such as debugging critical issues or fulfilling legal obligations.

3.2 User Access

- Each user is provided a unique API key.
- Users can only access documents under their own accounts.
- No user is granted access to another user's documents or data.

---

4. Access Management Procedures

4.1 Employee Onboarding

1. New employees are granted access based on their role.
2. All access to user data is disabled by default.
3. Developers are provisioned with development environment credentials only.

4.2 Privileged Access Management

1. Privileged API keys are only available to the two designated admins.
2. Privileged access is reviewed monthly to ensure compliance with the principle of least privilege.
3. Use of the privileged API key is logged and auditable.

4.3 User Key Management

1. API keys for users are automatically generated and issued at account creation.
2. Users are responsible for safeguarding their API keys.
3. API keys can be regenerated by the user through their account settings if compromised.

4.4 Access Reviews and Audits

1. **Employee Access Review**: Conducted quarterly to ensure that only necessary access is maintained.
2. **User Access Review**: Automated scripts run periodically to verify that users only have access to their own documents.
3. **Audit Logs**: All access to user data through privileged APIs is logged and reviewed for suspicious activity.

---

5. Incident Response

1. **Detection**: Unusual or unauthorized access is flagged through monitoring systems.
2. **Containment**: Immediate revocation of access for compromised accounts or employees.
3. **Investigation**: Admins will review logs to determine the scope and nature of the incident.
4. **Notification**: Affected users will be notified within 72 hours if their data is compromised.
5. **Recovery**: Steps will be taken to secure affected data and prevent recurrence.

---

6. Enforcement and Compliance

1. Employees found in violation of this policy will be subject to disciplinary action, up to and including termination.
2. Users violating the terms of access will have their accounts suspended and may be subject to legal action.

---

7. Responsibilities

- **Admins (Cofounders)**: Ensure policy adherence, manage privileged access, and conduct access audits.
- **Developers**: Ensure they only work with fake data and adhere to access restrictions.
- **Users**: Safeguard their API keys and report any suspicious activity.

---

8. Policy Review

This policy will be reviewed annually or when significant changes occur in the system architecture or legal requirements.

Approved by: Uri Merhav (CIO)
Effective Date: 10/01/2024
Next Review Date: 01/01/2025