Access Control Policy

Document creation Date:	June 15, 2025
Effective Date:	July 2, 2025
Version:	1.2
Classification:	Public

1. Purpose

This Access Control Policy establishes the principles, procedures, and technical controls used by Divy It Up, LLC (the "Company") to ensure that access to systems, data, and resources is granted only to authorized individuals and services on a need-to-know basis.

The policy enforces the principle of least privilege, strong authentication, and continuous monitoring across the Company's AWS-based backend infrastructure, applications, and integrations (including Plaid).

2. Scope

This policy applies to:

- All Company systems, applications, databases, and infrastructure (AWS backend)
- All users, employees, contractors, and service accounts
- All authentication and authorization mechanisms, including Amazon Cognito and AWS IAM
- All access tokens, API keys, encryption keys, and credentials
- All data classified as Internal or Sensitive under the Information Security Policy

3. Responsibilities

- **Security Team / CISO**: Owns policy implementation, access reviews, and exception approvals
- **Engineering / DevOps**: Implements and maintains IAM roles, Cognito configurations, and automated rotation
- **All Personnel**: Use only assigned credentials, report suspicious activity, and adhere to least privilege
- **Legal / Compliance**: Ensures access controls meet regulatory and contractual obligations

4. Principles of Access Control

The Company enforces the following core principles:

- **Least Privilege**: Users and services receive only the minimum permissions required
- **Role-Based Access Control (RBAC)**: Permissions are assigned via predefined roles rather than individual users
- **Separation of Duties**: No single individual can perform all steps of a critical process
- **Just-in-Time Access**: Temporary elevated privileges are used where possible
- **Zero Trust**: All access is verified, never assumed

5. Authentication

All access to Company systems requires strong, multi-factor authentication.

5.1 User Authentication – Amazon Cognito

- User authentication is managed via **Amazon Cognito User Pools**
- MFA is mandatory for all administrative and sensitive accounts
- Password policies enforce complexity, length, and history requirements
- Passwords are never stored in plaintext (hashed with industry-standard algorithms)

5.2 Service and Infrastructure Authentication – AWS IAM

- Infrastructure and backend services use **AWS IAM roles** with temporary credentials via AssumeRole
- Long-lived IAM access keys are prohibited for production workloads where possible
- All human access to AWS Console requires MFA

6. Authorization

Authorization decisions are made through a combination of Cognito and IAM.

- **Amazon Cognito Identity Pools** provide temporary AWS credentials to authenticated users and services
- **AWS IAM Policies** (managed and inline) enforce fine-grained permissions

- Resource-based policies and SCPs (Service Control Policies) are applied at the organization level where applicable

7. Access Tokens

- **JSON Web Tokens (JWTs)** are issued by Amazon Cognito upon successful authentication
- Access tokens are short-lived (default: 60 minutes) with automatic refresh token handling
- ID tokens and refresh tokens follow secure storage and transmission practices (HTTPS-only, HttpOnly cookies where applicable)
- Token validation occurs on every API request using Cognito JWT libraries and signature verification

8. Credential and Key Management

All credentials and cryptographic keys are managed securely using AWS native services.

8.1 Key Rotation Schedule

The Company enforces automated and manual rotation of keys and credentials according to the following schedule:

Credential / Key Type	Rotation Frequency	Method / Tool	Responsible Team
IAM User Access Keys	Every 90 days	Automated via AWS Lambda + Secrets Manager	DevOps
Cognito App Client Secrets	Every 90 days	Automated rotation scripts	Engineering
AWS KMS Customer-Managed Keys	Every 365 days	AWS KMS automatic rotation	Security Team
Database & API Credentials	Every 90 days	AWS Secrets Manager rotation	DevOps
Refresh Tokens (Cognito)	Session-based	Automatic invalidation on logout/expiry	Cognito Service

Credential / Key Type	Rotation Frequency	Method / Tool	Responsible Team
Long-lived Service Account Keys	Every 60 days (if used)	Manual + automated alerts	Security Team

Rotation events are logged, tested in staging, and trigger post-rotation validation.

9. Access Provisioning and De-Provisioning

- Access is provisioned only after formal approval and background checks (where applicable)
- Automated de-provisioning occurs immediately upon termination or role change
- All access changes are logged in AWS CloudTrail and centralized logging

10. Access Reviews and Auditing

- Quarterly access reviews are conducted for all privileged accounts
- Automated alerts notify managers of unused permissions
- AWS IAM Access Analyzer and Access Advisor are used to identify overly permissive roles

11. Monitoring and Logging

- All authentication and authorization events are logged via Amazon CloudTrail, CloudWatch, and Cognito logs
- Anomalous access attempts trigger real-time alerts to the Security Team
- Logs are retained per the Data Retention Policy

12. Exceptions and Temporary Access

Any exception to this policy requires written approval from the CISO and is time-bound (maximum 30 days). Temporary elevated access uses AWS IAM Just-in-Time permissions via AWS SSO or IAM roles.

13. Policy Review and Updates

This policy is reviewed annually or after any significant infrastructure, regulatory, or incident-related change. Updates are coordinated with the Information Security Policy.

14. Contact Information

Questions or access-related requests should be directed to:

Security Team

Divy It Up, LLC

security@divyitup.com

Revision History

Version	Date	Description	Author
1.0	July 2, 2025	Initial formal release	Security & Engineering Team