PURECHART

Access Control and Authentication Policy

Company: Purechart AI LLC
Effective Date: March 2026
Policy Owner: Technology and development team
Security Contact: security@purechart.com
Review Frequency: At least annually

---

1. Purpose

This Access Control and Authentication Policy establishes the requirements and procedures for controlling access to Purechart AI LLC's systems, applications, production environments, and sensitive data.

The purpose of this policy is to ensure that access is granted only to authorized individuals and systems based on legitimate business needs and appropriate security controls.

---

2. Scope

This policy applies to:

- Employees and contractors
- Production and non-production environments
- Cloud infrastructure and virtual assets
- Applications and databases
- Sensitive consumer and customer data
- Administrative accounts
- APIs and system integrations
- Service accounts and other non-human identities

PURECHART

3. Access Control Principles

Purechart follows the principles of:

- Least privilege
- Role-based access
- Need-to-know access
- Zero Trust security principles
- Separation of duties where applicable

Access to systems and sensitive information is granted only when necessary for an individual's job responsibilities or a system's authorized function.

---

4. Role-Based Access Control (RBAC)

Purechart uses Role-Based Access Control (RBAC) to manage access to systems, applications, and sensitive data.

Access permissions are assigned based on defined roles and job responsibilities.

Users are provided only the level of access necessary to perform authorized duties. Administrative and privileged access is restricted to authorized personnel.

Access roles and permissions may include:

- System administrators
- Developers
- Authorized support personnel
- Business users
- Standard application users

---

5. Authentication Requirements

Access to Purechart systems requires appropriate authentication.

Authentication controls include:

- Unique user accounts

- Secure password requirements
- Multi-factor authentication (MFA) for applicable systems
- Role-based authorization
- Secure session management

Shared credentials are prohibited except where technically necessary and specifically authorized.

---

6. Multi-Factor Authentication

Multi-factor authentication (MFA) is required for access to critical systems and sensitive environments where applicable.

This includes appropriate protection for:

- Administrative accounts
- Production infrastructure
- Cloud management systems
- Systems processing sensitive consumer data
- Other privileged or critical systems

MFA provides an additional layer of protection beyond usernames and passwords.

---

7. Production Access

Access to production assets, whether physical or virtual, is restricted to authorized personnel and systems.

Production access is granted based on:

- Legitimate business need
- Job responsibilities
- Required level of access
- Security considerations

Privileged production access is limited and monitored.

PURECHART

8. Periodic Access Reviews

Access permissions for production systems and sensitive data are periodically reviewed and audited.

Reviews are conducted to verify that:

- Access remains necessary
- Permissions remain appropriate
- Excessive privileges are identified
- Unauthorized access is removed
- Former employees or contractors no longer retain access

Access is modified when roles or responsibilities change.

---

9. Automated Provisioning and De-Provisioning

Purechart uses processes to manage the provisioning, modification, and removal of access.

Access is modified or removed when:

- An employee or contractor changes roles
- Access is no longer required
- Employment or contractual relationships end
- Unauthorized or unnecessary access is identified

Where supported by the applicable system, automated provisioning and de-provisioning mechanisms are used to ensure timely access changes.

---

10. Centralized Identity and Access Management

Purechart uses centralized identity and access management controls to manage authorized user identities and access permissions.

Centralized access management is used, where applicable, to:

- Manage user accounts
- Authenticate users

- Assign access permissions
- Enforce authentication requirements
- Modify access
- Disable or remove accounts

---

11. Zero Trust Architecture

Purechart applies Zero Trust security principles to access decisions involving systems and sensitive information.

No user, device, or system is automatically trusted solely based on network location or prior access.

Access decisions are based on appropriate verification of:

- Identity
- Authentication status
- Authorization level
- Role and permissions
- Requested resource
- Business need

Access to sensitive resources is continuously restricted according to applicable authorization controls.

---

12. Non-Human Authentication

Applications, APIs, services, and other non-human systems must use secure authentication mechanisms.

Approved mechanisms may include:

- OAuth tokens
- API access tokens
- TLS certificates
- Service accounts
- Other approved cryptographic authentication mechanisms

Secrets, tokens, certificates, and credentials must be protected against unauthorized access and must not be unnecessarily exposed in application code or unsecured locations.

---

13. Access Logging and Monitoring

Security-relevant access activities are logged and monitored where technically feasible.

This may include:

- Authentication events
- Failed login attempts
- Privileged access
- Administrative actions
- Changes to access permissions
- Access to sensitive systems

Suspicious or unauthorized access activity may be investigated and addressed according to Purechart's security incident procedures.

---

14. Access Revocation

Access must be promptly revoked or modified when:

- Employment ends
- A contractor's engagement ends
- A user changes roles
- Access is no longer required
- Unauthorized activity is suspected

Former personnel must not retain unnecessary access to company systems or sensitive data.

---

15. Policy Compliance

All employees, contractors, and authorized users must comply with this policy.

Unauthorized attempts to access systems, production assets, or sensitive information are prohibited and may result in removal of access privileges and other appropriate action.

---

16. Policy Review

This policy shall be reviewed periodically and updated when necessary, including following:

- Significant changes to infrastructure
- Changes in authentication technology
- Security incidents
- Changes in business operations
- New regulatory or contractual requirements