PURECHART

# Information Security Policy

**Document Title:** Information Security Policy
**Company:** Purechart AI LLC
**Effective Date:** March 2026
**Last Reviewed:** September 2026
**Policy Owner:** Technology and development team
**Security Contact:** security@purechart.com
**Review Frequency:** At least annually

---

## 1. Purpose

The purpose of this Information Security Policy is to establish the security principles, responsibilities, and practices used by Purechart AI LLC ("Purechart") to protect company systems, applications, infrastructure, and sensitive information.

Purechart is committed to protecting the confidentiality, integrity, and availability of information processed through its products and services, including customer, patient, business, and consumer financial information where applicable.

This policy establishes a framework for identifying, assessing, mitigating, and monitoring information security risks relevant to Purechart's business operations and technology environment.

---

## 2. Scope

This policy applies to:

- Purechart employees and contractors
- Company-owned and managed systems
- Production and non-production environments
- Cloud infrastructure
- Applications and databases
- APIs and third-party integrations

- Customer and consumer information
- Authentication credentials and secrets
- Company devices used to access business systems

This policy applies to all personnel who access Purechart systems or information.

---

## 3. Information Security Objectives

Purechart's information security program is designed to:

1. Protect sensitive information from unauthorized access or disclosure.
2. Protect the integrity and accuracy of information and systems.
3. Maintain the availability and reliability of production services.
4. Identify and mitigate information security risks.
5. Limit access to systems and data based on legitimate business needs.
6. Monitor systems for suspicious or unauthorized activity.
7. Respond appropriately to security incidents.
8. Regularly review and improve security practices.

---

# 4. Security Governance and Responsibilities

Purechart management is responsible for overseeing the company's information security program and ensuring appropriate security controls are implemented.

The designated security contact is responsible for coordinating information security matters, including:

- Security policy oversight
- Security risk identification
- Coordination of security reviews
- Security incident coordination
- Communication regarding security concerns
- Periodic review of security controls

Security inquiries may be directed to:

**Email:** security@purechart.com

All employees and contractors are responsible for following applicable security procedures and protecting company and customer information.

---

# 5. Risk Management

Purechart identifies and evaluates information security risks relevant to its business, technology, and data processing activities.

Security risks may include:

- Unauthorized access
- Data loss or disclosure
- Software vulnerabilities
- Compromised credentials
- Malware or malicious activity
- Third-party security risks
- Infrastructure failures
- Application security weaknesses

Identified risks are evaluated based on their potential impact and likelihood.

Appropriate measures may include:

- Technical security controls
- Access restrictions
- Encryption
- Security monitoring
- Software updates and patches
- Vulnerability remediation
- Changes to business procedures

Security risks and controls are reviewed periodically and when significant changes occur to the company's systems or services.

---

PURECHART

# 6. Access Control

Access to Purechart systems, production environments, and sensitive information shall be restricted to authorized individuals with a legitimate business need.

Purechart follows the principle of **least privilege**, meaning users should receive only the level of access necessary to perform their authorized responsibilities.

Access controls include, where applicable:

- Unique user accounts
- Role-based access control
- Authentication requirements
- Multi-factor authentication
- Administrative access restrictions
- Access logging
- Periodic review of privileged access

Shared accounts should be avoided whenever reasonably possible.

Access shall be modified or revoked when an individual's role changes or when access is no longer required.

---

# 7. Authentication and Multi-Factor Authentication

Purechart uses authentication controls to protect access to applications, infrastructure, and sensitive systems.

Where supported and appropriate, multi-factor authentication (MFA) is used to provide additional protection for access to critical systems.

MFA may be required for administrative or privileged access to systems containing sensitive information. Authentication credentials must be protected and must not be improperly shared with unauthorized individuals.

---

PURECHART

# 8. Protection of Data

Purechart implements reasonable technical and organizational measures to protect sensitive information.

Sensitive data protections include, where applicable:

- Encryption in transit
- Encryption at rest
- Access restrictions
- Authentication controls
- Audit logging
- Secure backups
- Monitoring and security alerts

Purechart limits access to sensitive information based on authorized business requirements.

---

# 9. Encryption

Purechart uses encryption to protect information during transmission and storage.

### Data in Transit

Communications between clients, applications, APIs, and servers are protected using secure encrypted connections, including TLS 1.2 or higher where applicable.

### Data at Rest

Sensitive data stored within supported systems and infrastructure is protected using appropriate encryption mechanisms.

Encryption controls are reviewed as technology and security requirements evolve.

---

PURECHART

# 10. Production Environment Security

Production systems contain critical applications and data and therefore require additional access controls.

Access to production environments shall be restricted to authorized personnel.

Production access should:

- Be granted only when necessary
- Follow the principle of least privilege
- Require appropriate authentication
- Be monitored and logged where technically feasible
- Be reviewed periodically

Development and testing activities should be appropriately separated from production operations whenever practical.

---

# 11. Vulnerability Management

Purechart maintains processes intended to identify and address security vulnerabilities affecting company systems and applications.

Security practices may include:

- Monitoring for known vulnerabilities
- Vulnerability scanning
- Security assessments
- Dependency monitoring
- Software updates
- Security patching
- Third-party penetration testing where appropriate

Security vulnerabilities are evaluated based on their potential severity and impact.

Critical security vulnerabilities should be prioritized for remediation.

---

PURECHART

# 12. Security Monitoring and Logging

Purechart maintains logging and monitoring capabilities designed to identify security-relevant events.

Where applicable, security monitoring may include:

- Authentication activity
- Failed login attempts
- Administrative activity
- Access to sensitive systems
- Changes to system configurations
- Suspicious or anomalous activity

Security events may be investigated and escalated based on their severity and potential impact.

---

# 13. Secure Software Development

Purechart incorporates security considerations into the development and maintenance of its software.

Security practices may include:

- Authentication and authorization controls
- Secure API development
- Code review
- Dependency management
- Security testing
- Protection of credentials and secrets
- Vulnerability remediation

Changes to production systems should be reviewed and tested according to appropriate development procedures.

---

PURECHART

# 14. Third-Party Services and Integrations

Purechart uses third-party providers and technology services to support its business and application infrastructure.

Third-party integrations that process sensitive information should be evaluated based on their security and business requirements.

Access credentials, API keys, tokens, and secrets used for third-party services must be protected from unauthorized access.

Third-party access should be limited to what is necessary for the applicable service.

---

# 15. Consumer Financial Data

Where Purechart processes consumer financial information through authorized third-party integrations, including Plaid, such information shall be handled with appropriate security controls.

Purechart will:

- Limit access to authorized personnel and systems
- Use encrypted communications
- Protect stored sensitive data where applicable
- Limit collection and retention to legitimate business purposes
- Use secure authentication mechanisms
- Protect API credentials and access tokens
- Follow applicable contractual and legal requirements

Purechart should avoid storing sensitive financial information unless necessary for the intended business purpose.

---

PURECHART

# 16. Incident Response

Purechart maintains procedures for responding to suspected security incidents.

A security incident may include:

- Unauthorized access
- Suspected data breach
- Compromised credentials
- Malware or malicious activity
- Loss of sensitive information
- Security system compromise

When a security incident is identified, appropriate personnel shall assess the situation and take reasonable steps to:

1. Identify the incident.
2. Contain the issue.
3. Investigate the potential impact.
4. Remediate the vulnerability or security issue.
5. Restore affected services where necessary.
6. Document the incident and corrective actions.

Notifications will be handled in accordance with applicable legal, regulatory, and contractual requirements.

---

# 17. Data Retention and Deletion

Purechart retains information only for as long as reasonably necessary to provide services, meet legitimate business requirements, comply with legal obligations, and maintain appropriate records.

When data is no longer required, it should be securely deleted or de-identified in accordance with applicable procedures and technical capabilities.

Data retention practices shall be periodically reviewed.

---

PURECHART

# 18. Privacy and Consumer Consent

Purechart maintains privacy practices governing the collection, processing, storage, and use of personal information.

Where required, consumers shall be provided appropriate notice and consent mechanisms regarding the collection and processing of their information.

Purechart's public-facing Privacy Policy provides additional information regarding applicable privacy practices.

---

# 19. Security Awareness

Personnel with access to company systems and sensitive information are expected to follow applicable security practices.

Personnel should:

- Protect passwords and authentication credentials
- Avoid sharing credentials
- Report suspected security incidents
- Follow access control requirements
- Protect sensitive information
- Use company systems responsibly

---

# 20. Policy Compliance

Failure to comply with this Information Security Policy may result in the removal of system access or other appropriate corrective actions.

Personnel are expected to report suspected violations or security concerns to appropriate management or the designated security contact.

---

PURECHART

# 21. Policy Review and Updates

This policy shall be reviewed at least annually and updated when necessary.

Reviews may also occur following:

- Significant security incidents
- Major changes to infrastructure
- Significant changes to business operations
- New regulatory requirements
- New third-party integrations
- Changes in information security risks

---