Data Security & Protection

Vested Property Care
Effective Date: April 12, 2026

Executive Summary

Vested Property Care is committed to protecting customer data through industry-standard security practices, encryption, access controls, and compliance with applicable regulations. This document outlines the technical and operational measures we implement to safeguard your information.

---

1. Authentication & Session Management

OAuth 2.0 Authentication

Customers authenticate through a secure third-party OAuth provider (Manus), which means:

- Your password is never shared directly with Vested Property Care
- We receive a secure authentication token instead of your credentials
- Reduces the risk of password breaches on our infrastructure
- Complies with OAuth 2.0 industry standards

Session Cookies

After successful authentication, a secure session cookie is created with the following protections:

- **HttpOnly flag** — Prevents JavaScript from accessing the cookie (protects against XSS attacks)

- **Secure flag** — Cookie only transmits over HTTPS, never over unencrypted HTTP
- **SameSite attribute** — Prevents cross-site request forgery (CSRF) attacks
- **Automatic expiration** — Sessions expire after a defined period, requiring re-authentication

JWT Tokens

Session tokens are cryptographically signed and verified by our server:

- Tokens cannot be forged or modified without the signing secret
- Each request validates the token signature before granting access
- Expired tokens are automatically rejected

---

2. Data Encryption

In Transit (HTTPS/TLS)

All communication between your browser and our servers is encrypted using TLS 1.2 or higher:

- Encrypts all data traveling over the internet (addresses, property details, service requests)
- Prevents eavesdropping and man-in-the-middle attacks
- Your browser displays a padlock icon (🔒) indicating a secure connection
- Certificates are issued by trusted certificate authorities

At Rest (Database)

Sensitive data stored in our database is protected through:

- **Database isolation** — Your data is isolated to your account only
- **Access controls** — Only authorized application code can access the database
- **No direct internet access** — The database is not exposed to the public internet

- **Encryption at storage layer** — Database encryption is managed by our hosting provider

API Keys & Secrets

All sensitive credentials are protected:

- Stored as **environment variables**, never in source code
- Never logged or displayed in error messages
- Only accessible to the server runtime
- Rotated periodically per security best practices

---

3. Payment Security

PCI-DSS Compliance

Vested Property Care does not store, process, or transmit credit card information. Instead:

- All payment processing is handled by **Stripe**, a PCI-DSS Level 1 certified payment processor
- Your credit card information never reaches our servers
- We store only a secure reference (token) to your payment method
- Stripe handles all card data encryption and security

Tokenization

Credit cards are converted to secure tokens:

- Tokens (e.g., `pm_xxxxx`) are safe to store and reference
- Actual card data remains encrypted within Stripe's secure infrastructure
- Tokens cannot be reversed to reveal card numbers

Webhook Verification

When Stripe sends payment notifications to our system:

- We verify the cryptographic signature to ensure the webhook came from Stripe
- Prevents attackers from sending fake payment confirmations
- Only legitimate payment events are processed

---

4. Database Security

SQL Injection Prevention

Our application uses an Object-Relational Mapping (ORM) system that:

- Automatically parameterizes all database queries
- Prevents user input from being interpreted as SQL code
- Validates all input before database operations
- Example: User input is treated as data, never as executable code

Access Control

Database access is restricted through:

- **Role-based access** — Different user roles have different permissions
- **Data ownership** — Customers can only access their own data
- **Admin procedures** — Admin-only operations require role verification
- **Principle of least privilege** — Users have minimum necessary permissions

Backup & Recovery

Your data is protected through:

- Regular automated backups
- Secure backup storage
- Disaster recovery procedures

- Data retention policies compliant with applicable laws

---

5. API Security

Protected Endpoints

All customer data endpoints require authentication:

- Unauthenticated requests are rejected with an error
- Session cookie is verified on every request
- Expired or invalid sessions are denied access

Role-Based Access Control (RBAC)

Access to sensitive operations is restricted by user role:

- **Customer role** — Can view/edit only their own properties and service requests
- **Admin role** — Can access customer accounts, service requests, and reports (with audit logging)
- **Vendor role** — Can view assigned work orders and submit completion data
- Each role has specific permissions enforced at the API level

Input Validation

All incoming data is validated before processing:

- Data type checking (e.g., phone numbers are formatted correctly)
- Length validation (e.g., addresses don't exceed reasonable limits)
- Format validation (e.g., email addresses are valid)
- Invalid requests are rejected before reaching the database

Rate Limiting

API endpoints are protected against abuse:

- Excessive requests from a single user are throttled
- Prevents brute-force attacks and denial-of-service attempts
- Legitimate users are not affected

---

6. Data Privacy & Separation

Document Vault (Personal)

Your personal documents remain with you:

- Only you can access your Document Vault
- Contents include: insurance documents, financial records, personal notes
- Automatically deleted when your account is closed
- Does NOT transfer to the next property owner

Vested Home Record (Property-Based)

Your property's maintenance history remains with the property:

- Includes: service logs, vendor information, maintenance dates, repair receipts
- Transfers to the next property owner when you sell
- Provides lasting value to the property
- You can review and remove personal items before property transfer

Data Minimization

We collect and store only the data necessary to provide services:

- Name, email, phone number
- Property addresses and details
- Service request history
- Credit balance and transaction history

- We do NOT store: social security numbers, driver's license numbers, full credit card numbers

---

7. Third-Party Security

Manus OAuth Provider

- Handles secure authentication
- Manages OAuth credentials and tokens
- Complies with OAuth 2.0 standards
- Security certifications and compliance verified

Stripe Payment Processing

- PCI-DSS Level 1 certified
- Handles all credit card data
- Fraud detection and prevention
- Complies with payment card industry standards

Twilio SMS Service

- Handles SMS delivery for vendor work order links
- Credentials stored securely in environment variables
- SMS content does not include sensitive personal information
- Complies with telecommunications regulations

Manus Cloud Infrastructure

- Provides hosting, database management, and SSL/TLS certificates
- Manages server security, firewalls, and DDoS protection
- Regular security audits and compliance certifications
- Automatic backups and disaster recovery

---

8. Logging & Monitoring

Audit Trails

Important actions are logged for security and compliance:

- User login/logout events
- Administrative actions (e.g., credit adjustments, vendor assignments)
- Service request creation and status changes
- Payment transactions

Sensitive Data Exclusion

Our logs do NOT include:

- Passwords or authentication tokens
- Credit card numbers or payment details
- API keys or secrets
- Personal identification numbers

Monitoring & Alerts

We monitor for suspicious activity:

- Multiple failed login attempts
- Unusual access patterns
- Unauthorized administrative actions
- Database anomalies

---

9. Compliance & Legal

Applicable Regulations

Vested Property Care complies with:

- **GDPR** (General Data Protection Regulation) — If you're in the EU
- **CCPA** (California Consumer Privacy Act) — If you're in California
- **HIPAA** — Not applicable (we don't handle health information)
- **PCI-DSS** — Through our Stripe integration
- **State privacy laws** — Including Florida's data protection requirements

Data Rights

You have the right to:

- **Access** — Request a copy of your personal data
- **Correction** — Update or correct inaccurate information
- **Deletion** — Request deletion of your data (subject to legal retention requirements)
- **Portability** — Receive your data in a portable format
- **Opt-out** — Unsubscribe from non-essential communications

To exercise these rights, contact us at **info@vestedpropertycare.com** or **(941) 336-5116**.

Data Retention

We retain customer data:

- **Active accounts** — For the duration of your subscription
- **Closed accounts** — For 7 years (tax and legal compliance requirements)
- **Vested Home Records** — Retained indefinitely with the property address
- **Payment records** — Retained per PCI-DSS and tax requirements

Incident Response

In the event of a security incident:

- We investigate the scope and impact
- We notify affected customers without unreasonable delay

- We cooperate with law enforcement if necessary
- We implement corrective measures to prevent recurrence

---

10. Security Best Practices for Customers

To protect your account, we recommend:

✅ **DO:**

- Use a strong, unique password for your account
- Enable two-factor authentication if available
- Log out when using shared computers
- Keep your browser and operating system updated
- Report suspicious activity immediately
- Review your account activity regularly
- Use HTTPS connections (look for the padlock icon)

❌ **DON'T:**

- Share your login credentials with anyone
- Use the same password across multiple websites
- Log in on public WiFi without a VPN
- Click suspicious links in emails
- Download files from untrusted sources
- Leave your browser logged in on shared computers
- Ignore security warnings from your browser

---

11. Security Certifications & Standards

Vested Property Care and its service providers maintain:

- **TLS 1.2+** encryption for all data in transit

- **OAuth 2.0** compliance for authentication
- **PCI-DSS Level 1** compliance through Stripe (payment processing)
- **SOC 2 Type II** compliance through our hosting provider
- Regular security audits and penetration testing

---

12. Contact & Questions

If you have questions about our security practices or data protection:

Email: info@vestedpropertycare.com
Phone: (941) 336-5116
Website: vestedpropertycare.com

For urgent security concerns, please contact us immediately.

---

13. Document History

Version	Date	Changes
1.0	April 12, 2026	Initial document

Disclaimer

This document describes our current security practices and is provided for informational purposes. While we implement industry-standard security measures, no system is completely immune to security risks. We continuously update our security practices to address emerging threats and comply with applicable regulations.

For legal terms governing your use of our services, please refer to our **Terms of Service** and **Privacy Policy** available on our website.

Last Updated: April 12, 2026
Vested Property Care

Venice, Florida