

PatrolPlan Pro

Service Definition Document

Version 1.0 | January 2026

Digital Web Media Ltd
Barn Owl Cottage, Chapel Hill, Ponsanooth, Cornwall, TR3 7ET
Company Number: 8649718

All prices are in GBP and exclude VAT

Contents

1. What the Service Is	4
1.1 Service Overview	4
1.2 Core Capabilities	4
1.3 Emergency Equipment Locator	4
1.4 Platform Access	5
1.5 Target Sectors	5
2. Data Backup and Disaster Recovery	6
2.1 Backup Schedule	6
2.2 Geographic Redundancy	6
2.3 Recovery Objectives	6
2.4 Business Continuity	6
3. Onboarding and Offboarding Support	6
3.1 Implementation	7
3.2 Standard Onboarding	7
3.3 Professional Services	7
3.4 Contract Exit	7
4. Service Constraints	7
4.1 Maintenance Windows	7
4.2 Customisation	7
4.3 Usage Limits	8
5. Service Levels	8
5.1 Availability	8
5.2 Service Credits	8
5.3 Performance	8
5.4 Support Hours	8
6. After Sales Support	9
6.1 Support Channels	9
6.2 Issue Priority	9
6.3 Included Updates	9
7. Technical Requirements	9
7.1 Mobile Devices	9
7.2 Web Portal	10
7.3 Network	10
7.4 Integration	10
8. Outage and Maintenance Management	10
8.1 Planned Maintenance	10
8.2 Unplanned Outages	10
8.3 Incident Management	10
9. Hosting Options and Locations	11
9.1 Infrastructure	11
9.2 Data Sovereignty	11
9.3 Data Centre Security	11
10. Access to Data Upon Exit	11
10.1 Data Export	11
10.2 Export Formats	11
10.3 Post-Termination	11
11. Security	11
11.1 Certifications	12
11.2 Encryption	12

11.3 Access Control.....	12
11.4 Application Security	12
11.5 Audit	12
11.6 Personnel.....	12
12. Contact Information	13

1. What the Service Is

1.1 Service Overview

PatrolPlan Pro is a cloud-based security patrol management system designed for the UK public sector. The platform enables organisations to manage security personnel, verify checkpoint attendance through GPS, coordinate teams in real-time, and maintain comprehensive audit trails for regulatory compliance.

Built with an offline-first architecture, PatrolPlan Pro ensures frontline staff can continue working effectively even in areas with poor connectivity, with all data automatically synchronising when connection is restored.

1.2 Core Capabilities

The platform delivers the following features:

- GPS-verified check-ins with configurable radius validation to confirm physical presence at checkpoints
- Biometric authentication (Face ID and fingerprint) for secure mobile app access
- Offline-first mobile application ensuring continuous operation without network connectivity
- Automatic data synchronisation when connectivity is restored
- What3Words integration for precise emergency location communication
- Checkpoint objectives allowing staff to confirm specific tasks completed at each location
- Notes capture on check-ins for recording observations or issues
- Real-time team visibility showing staff locations for supervisors
- Emergency contact directory with one-tap calling
- Resource directory with categorised local services and facilities
- Interactive mapping using OpenStreetMap
- Event-based access codes for temporary staff and contractors

1.3 Emergency Equipment Locator

PatrolPlan Pro includes a dedicated emergency equipment location feature, enabling staff to quickly locate life-saving equipment during critical incidents. All emergency equipment is displayed on the interactive map with real-time distance calculations from the user's current GPS position.

Defibrillator (AED) Locations

Registered Automated External Defibrillator locations are displayed on the interactive map. Staff can instantly identify the nearest AED to their current position, with distance calculated in real-time using GPS.

- Map display of all registered AED locations with distinctive icons
- Automatic identification of nearest defibrillator based on current GPS position
- Distance and walking directions to nearest unit
- Location details including building, floor, and access instructions

- One-tap navigation to selected defibrillator

Bleed Kit Locations

Public Access Bleed Kits (Bleed Control Kits) are increasingly deployed alongside defibrillators following the introduction of Daniel's Law. PatrolPlan Pro displays all registered bleed kit locations, enabling rapid response to serious bleeding emergencies.

- Map display of registered bleed kit locations with distinctive icons
- Automatic identification of nearest bleed kit based on current GPS position
- Distance and walking directions to nearest kit
- Location details and access information
- One-tap navigation to selected bleed kit

The emergency equipment locator is accessible from the main map view and from the dedicated Emergency screen, ensuring rapid access when time is critical. The 'Find Nearest' feature provides instant access to the closest defibrillator, bleed kit, and other critical resources.

1.4 Platform Access

PatrolPlan Pro is accessible through:

- iOS mobile application (iPhone and iPad)
- Android mobile application
- Web-based administration portal for management and reporting
- RESTful API for integration with existing organisational systems

1.5 Target Sectors

The platform is designed for organisations requiring verifiable patrol management:

Events and Festivals

Large-scale events require rapid deployment with temporary workforces. PatrolPlan Pro's event-specific model allows rapid checkpoint configuration and temporary access codes for stewards and security staff.

- Rapid deployment for temporary events
- Share codes for temporary staff access without full accounts
- What3Words integration for emergency response coordination
- Emergency equipment locations (defibrillators, bleed kits) for first responders
- Offline capability for areas with poor mobile coverage

Local Authorities

Council security teams can manage patrols across car parks, parks, civic buildings, and housing estates. The platform provides evidence of patrol coverage for insurance and compliance purposes.

- Multi-site patrol management
- Audit trail for duty of care demonstration

- Resource directory for local services
- Defibrillator and bleed kit location tracking for public spaces

Private Security

Security contractors can demonstrate service delivery to clients through verified check-in records with GPS timestamps.

- Verifiable patrol records for client reporting
- GPS evidence of checkpoint attendance
- Offline operation for sites with limited connectivity

2. Data Backup and Disaster Recovery

2.1 Backup Schedule

PatrolPlan Pro implements a comprehensive backup strategy:

- Full database backups performed daily at 02:00 UTC
- Incremental backups every 4 hours
- Transaction logs backed up every 15 minutes
- Backups retained for minimum 90 days
- All backups encrypted using AES-256

2.2 Geographic Redundancy

- Primary hosting in AWS eu-west-2 (London)
- Synchronous replication to secondary availability zone
- Backup storage in geographically separate UK data centre
- All data remains within United Kingdom

2.3 Recovery Objectives

Recovery Time Objective (RTO): 4 hours maximum to restore full service following a major incident.

Recovery Point Objective (RPO): 15 minutes maximum data loss, reflecting transaction log backup frequency.

2.4 Business Continuity

- Multi-availability zone deployment
- Automatic scaling for traffic fluctuations
- Database clustering with automatic failover
- Mobile app offline functionality during service disruptions
- Quarterly disaster recovery testing

3. Onboarding and Offboarding Support

3.1 Implementation

Each implementation includes a dedicated implementation manager. Typical deployments complete within two to four weeks.

3.2 Standard Onboarding

- Requirements gathering workshop
- Tenant environment provisioning (2 business days)
- System configuration including checkpoints and user roles
- Administrator training (remote, up to 2 hours)
- User documentation and training materials
- Go-live support
- Two-week hypercare period

3.3 Professional Services

Additional services available:

- On-site implementation support
- Extended training programmes
- Data migration from legacy systems
- Custom integration development

3.4 Contract Exit

- 30 days notice required
- Full data export in standard formats (CSV, JSON, PDF)
- Data retained 30 days post-termination
- Deletion confirmation available on request

4. Service Constraints

4.1 Maintenance Windows

- Standard window: Sundays 02:00-06:00 UTC
- Minimum 7 days advance notice
- Mobile app continues offline during maintenance

4.2 Customisation

Can be customised:

- Organisation branding
- Checkpoint types and validation rules
- User roles and permissions
- Report templates
- Emergency equipment categories

Cannot be customised:

- Core application architecture
- Security mechanisms
- Encryption standards
- Audit logging

4.3 Usage Limits

- API rate limits: 1,000 requests per minute
- File upload maximum: 25MB
- Data retention: Configurable up to 7 years

5. Service Levels

5.1 Availability

Target availability: 99.9% measured monthly (excluding scheduled maintenance).

5.2 Service Credits

Service credits are applied when availability targets are not met:

Monthly Availability	Service Credit
99.9% or above	No credit
99.0% to 99.89%	10% of monthly fee
95.0% to 98.99%	25% of monthly fee
Below 95.0%	50% of monthly fee

Credits are applied to the following month's invoice upon written request within 30 days.

5.3 Performance

- Web portal page load: Under 3 seconds
- API response time: Under 500ms
- Mobile sync: Under 10 seconds
- Check-in processing: Under 2 seconds

5.4 Support Hours

Standard Support:

- Monday to Friday: 09:00-17:30 UK time

- Email and ticket support
- Response within 8 business hours

Enhanced Support (optional):

- 7 days: 07:00-22:00 UK time
- Telephone support
- Response within 4 hours
- Named account manager

6. After Sales Support

6.1 Support Channels

- Email: support@patrolplan.com
- Online ticket portal
- Telephone (Enhanced Support)
- Knowledge base

6.2 Issue Priority

Issues are categorised by priority with corresponding response and resolution targets:

Priority	Description	Response	Resolution
P1 Critical	Service unavailable	1 hour	4 hours
P2 High	Major impact	4 hours	8 hours
P3 Medium	Minor impact	8 hours	5 days
P4 Low	Query	2 days	Scheduled

6.3 Included Updates

- Software updates at no additional cost
- Security patches applied automatically
- Bug fixes prioritised by impact

7. Technical Requirements

7.1 Mobile Devices

iOS Requirements:

- iOS 14.0 or later
- iPhone 8 or later recommended
- 100MB storage

Android Requirements:

- Android 10 or later
- 3GB RAM recommended
- Google Play Services required
- 100MB storage

7.2 Web Portal

- Modern browser (Chrome, Firefox, Safari, Edge - latest two versions)
- JavaScript enabled
- Minimum 1280x720 resolution

7.3 Network

- HTTPS access on port 443
- Mobile data or WiFi for synchronisation
- Offline mode available when disconnected

7.4 Integration

- RESTful API with JSON
- OAuth 2.0 authentication
- TLS 1.2 or later
- Webhook support

8. Outage and Maintenance Management**8.1 Planned Maintenance**

- Standard window: Sundays 02:00-06:00 UTC
- 7 days advance notice
- Typical duration under 2 hours
- Mobile offline available throughout

8.2 Unplanned Outages

- Real-time status at status.patrolplan.com
- Email notifications to administrators
- Post-incident report within 5 business days

8.3 Incident Management

- 24/7 automated monitoring
- On-call engineering team
- Hourly updates during P1 incidents

9. Hosting Options and Locations

9.1 Infrastructure

- AWS eu-west-2 (London) exclusively
- Multi-availability zone deployment
- All data stored and processed in UK
- No international data transfers

9.2 Data Sovereignty

- UK GDPR compliant
- UK legal jurisdiction
- Suitable for OFFICIAL classification

9.3 Data Centre Security

- ISO 27001, ISO 27017, ISO 27018 certified
- SOC 1, SOC 2, SOC 3 compliant
- Physical security with biometric access

10. Access to Data Upon Exit

10.1 Data Export

Full data export available at any time through the administration portal:

- Check-in records with timestamps and GPS coordinates
- User accounts and team structures
- Checkpoint configurations
- Emergency equipment locations (defibrillators, bleed kits)
- Audit logs

10.2 Export Formats

- CSV for tabular data
- JSON for structured data
- PDF for formatted reports

10.3 Post-Termination

- Data retained 30 days after contract end
- Complete deletion after retention period
- Deletion certification on request

11. Security

11.1 Certifications

- Cyber Essentials certified
- OWASP security guidelines followed
- Annual penetration testing
- GDPR compliant

11.2 Encryption

- Data at rest: AES-256
- Data in transit: TLS 1.2 minimum
- Encrypted backups

11.3 Access Control

- Role-based access control
- Biometric authentication on mobile (Face ID and fingerprint)
- Automatic session timeout
- Password complexity requirements

11.4 Application Security

- Secure development lifecycle
- Code review and static analysis
- Dependency vulnerability scanning
- Web Application Firewall

11.5 Audit

- Comprehensive activity logging
- Tamper-evident audit trails
- 12-month log retention minimum

11.6 Personnel

- Background checks for staff with data access
- Security awareness training
- Principle of least privilege

12. Contact Information

For enquiries regarding this service:

Digital Web Media Limited

Website: www.patrolplan.com

Email: sales@patrolplan.com

Document Version: 1.0

Last Updated: January 2026