



→ www.boris-software.com

FIELD SERVICE & FIRE-COMPLIANCE MANAGEMENT PLATFORM

BORIS SERVICE DEFINITION DOCUMENT

Streamline audits, workflows, assets, and reporting across every sector—all in one cloud-based platform.

1. Service Overview



BORIS is a cloud-based field service and compliance management platform used across fire stopping, fire doors, utilities, HVAC, and construction sectors. The service enables organisations to manage site audits, workforce operations, certification workflows, asset management, forms, checklists, reporting, and customer communication in a single unified platform.

The platform provides:

✓ **Field data capture via mobile and tablet**

✓ **Work order management**

✓ **Workforce scheduling and dispatch**

✓ **Fire-stopping and fire-door compliance recording**

✓ **Asset and equipment tracking**

✓ **Digital forms and workflows**

✓ **Customer portal and reporting**

✓ **Document and media storage**

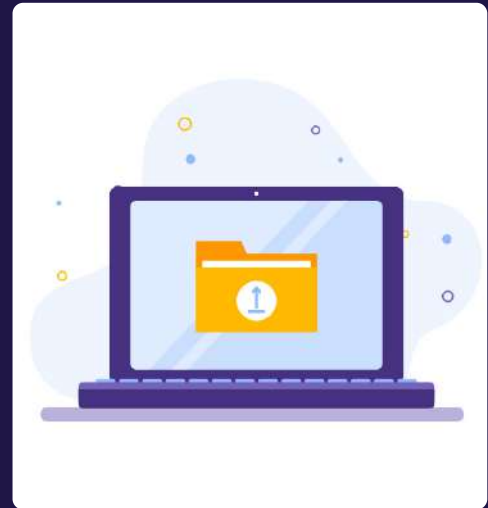
✓ **Integration with third-party systems (via API)**

BORIS is delivered as a fully managed SaaS offering.

2. Data Backup, Restore & Disaster Recovery

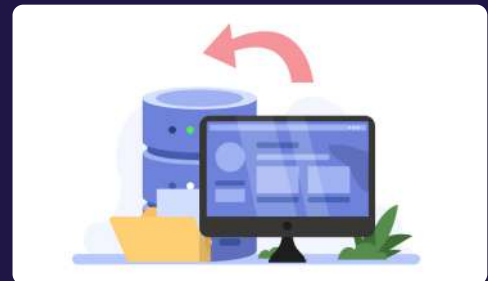
Backup Strategy

- **Database Backups:** Automated full backups daily, differential backups every 12 hours, and transactional log backups every 5 minutes.
- **Blob/File Storage:** Replicated across Azure storage with geo-redundant backup (GRS).
- **Retention Period:** 30-day default retention for production backups.
- **Encryption:** Backups are encrypted using Azure SQL Server TDE.



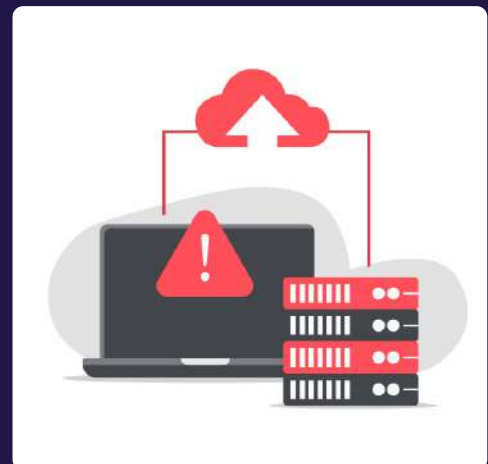
Restore Procedures

- Point-in-time restore capability for databases.
- Recovery of file storage via Azure blob snapshots.
- Restore tests conducted quarterly.



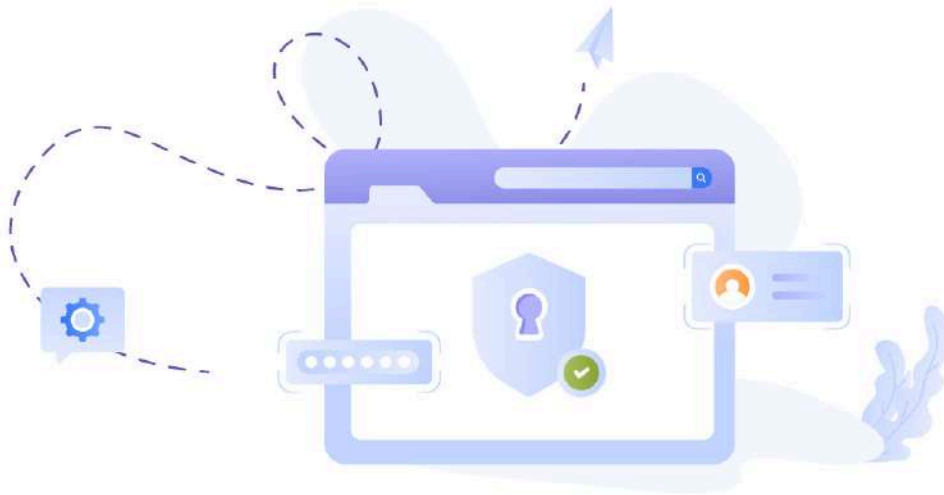
Disaster Recovery

- Hosted across **Azure UK South / UK West** with failover capability.
- RTO (Recovery Time Objective): **12 hours**
- RPO (Recovery Point Objective): **≤ 2 hours**
- DR plan includes full environment recreation scripts (IaC) and automated system provisioning workflows.



3. Onboarding & Offboarding Support

Onboarding



- Setup of customer environment (database provisioning, storage configuration, API keys).
- Configuration of modules (CRM, fire stopping, workforce, assets, etc.).
- User access setup and MFA configuration.
- Customer-specific training (remote workshops and documentation).
- Optional migration assistance for legacy data.

Offboarding

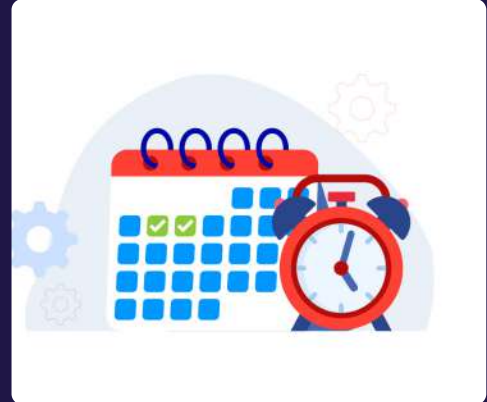
- Export of customer data (database export in CSV format, asset files, images, documents).
- Deactivation of accounts and removal of access.
- Data retention for 12 months unless otherwise contractually agreed.
- Full environment deletion after retention period.



4. Service Constraints

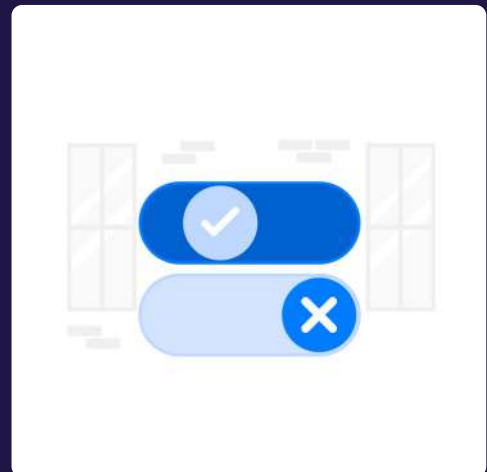
Maintenance Window:

- Regular weekly maintenance:
Sundays 00:00–04:00 UK Time
- Emergency maintenance may occur outside this window, with advance notice where possible.



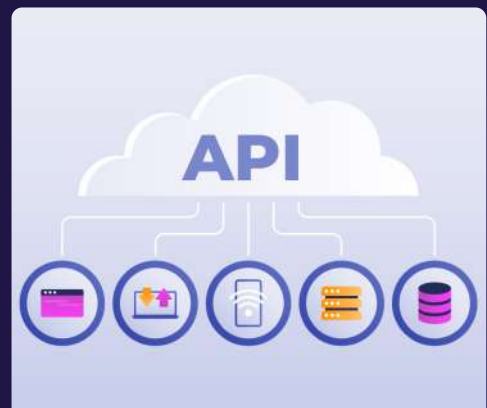
Customisation Limits:

- Core platform functionality is standardised across all customers.
- Allowed customisations include: forms, workflows, user roles, dashboards, integrations, and templates.
- Code-level modifications are not supported.



API Usage:

- API rate limits may apply to preserve service performance.
- Integrations must follow BORIS security standards (OAuth / API Key).



5. Service Levels (Performance, Availability & Support Hours)

Availability

- Target uptime: **99.5%** per calendar month (excluding planned maintenance).

Performance

- API responses: <500ms for standard operations.
- Dashboard loads optimised for sub-2 second load where dataset sizes permit.



Support Hours

- Standard Support: **Monday–Friday, 9am–5pm UK time**
- Critical Incident Support: **24/7**
- Support Channels: Email, helpdesk portal, phone for urgent issues.

6. After Sales Support

- Dedicated customer success manager (CSM).
- Ticketing via BORIS Helpdesk (Zoho Desk).
- Incident management following ITIL principles.
- Release notes provided for all deployments.
- Quarterly product review sessions (optional).
- Optional premium support package with prioritised response times.

7. Technical Requirements



- Dedicated customer success manager (CSM).
- Ticketing via BORIS Helpdesk (Zoho Desk).
- Incident management following ITIL principles.
- Release notes provided for all deployments.
- Quarterly product review sessions (optional).
- Optional premium support package with prioritised response times.

8. Outage & Maintenance Management

- Outage notifications sent via email or customer portal.
- Monitoring powered by Azure Monitor, Application Insights, and Azure WAF.
- Automated alerting for:
 - High error rates
 - Unresponsive APIs
 - Storage thresholds
 - Queue processor failures
- Root cause analysis (RCA) provided for Sev-1 and Sev-2 incidents.

9. Hosting Options & Locations

BORIS is hosted exclusively on **Microsoft Azure**.

Hosting Regions

- **Primary:** UK South
- **Secondary (Failover):** UK West

Infrastructure

- Azure SQL Server
- Azure VM-based hosting
- Azure Blob Storage
- Azure WAF
- Azure Virtual Network and Private Endpoints

Compliance

- TLS 1.2+ encryption
- MFA enforced
- Audit logs maintained in compliance with ISO 27001
- Bi-annual penetration testing

10. Access to Data (Upon Exit)

Customers may request their data in industry-standard formats.

Data Provided

- Database tables exported into CSV
- Media files exported from blob storage
- FRA templates and configuration files
- Audit logs (upon request)

Method

- Secure download from Azure Blob Storage or SFTP
- Data retained for 12 months post-termination unless otherwise agreed

11. Security

Data Security

- TLS 1.2+ encryption in transit
- Azure SQL encryption at rest (TDE)
- Role-based access control (RBAC)
- MFA available for all accounts
- Password rules based on NCSC recommendations
- Automated security patching for infrastructure



Access Controls

- Internal access restricted to authorised Boris Security & Infrastructure staff only
- Access granted only for support or maintenance with customer approval
- Audit logs for all administrative actions



Vulnerability Management

- Bi-annual penetration tests
- Monthly vulnerability scans



Network Security

- Azure WAF protecting APIs
- Private endpoints for internal modules
- IP allowlisting for administrative endpoints

