IPLICIT BACKUP POLICY

Effective Date: 1 September 2025
Version: 1.2

1. PURPOSE AND SCOPE

This Backup Policy outlines our commitment to data protection and business continuity for all customer data stored within iplicit. This policy applies to all customer data, system configurations, and critical business information processed through our services. The iplicit ecosystem is fully hosted on Microsoft Azure ("Azure"), leveraging its enterprise-grade infrastructure for security, resilience, and scalability. All data is managed using Azure SQL Database – which has some of the most extensive business continuity and disaster recovery measures available. For more detailed information on how Azure protects your data, please refer to Microsoft's official documentation by clicking the link below: https://docs.microsoft.com/en-us/azure/sql-database/sql-database-security-overview

2. BACKUP OBJECTIVES

Iplicit's backup strategy is designed to:

- Ensure business continuity and minimal service disruption
- Protect against data loss from system failures, human error, or security incidents
- Meet regulatory compliance requirements
- Maintain data integrity and availability
- Support disaster recovery operations

3. BACKUP TYPES AND FREQUENCY

Our backup strategy employs a multi-tiered approach, incorporating Point-in-Time Restore, Weekly, Monthly, and Yearly backups, along with Active Data-Replication, to ensure comprehensive data protection.

3.1 Production Environment Backups

Backup Type	Frequency	Retention Period	Description
Point-in-Time Restore	Continuous	14 Days	Enables restoration of databases to any point in time within the past 14 days
Weekly Backup Retention	Weekly	12 weeks	Weekly full backups are retained for 12 weeks, providing intermediate recovery points

Monthly Backup Retention	Monthly	24 months	Monthly full backups are retained for 24 months, allowing for longer-term data recovery options
Yearly Backup Retention	Yearly	7 years	Yearly full backups are retained for a period of 7 years, ensuring compliance with long-term data retention requirements

Sandboxes are only set-up with 7 days Point in Time Restore

3.3 Active Data-Replication

- **Included:** As Standard for all production environments
- **Description:** We continuously keep a live copy of your data in a physically separate location. This ensures your service stays running and available, even in the event of a major outage at one of our data centres.
- **Coverage:** Continuous replication of critical data to a separate Azure data centre

4. BACKUP STORAGE AND RETENTION

4.1 Total Backup Retention

- **Total Full Backups Retained:** 43 full backups at any given time
- **Composition:** Inclusive of weekly, monthly, and yearly backups as detailed in the backup schedule above
- **Storage Infrastructure:** Microsoft Azure cloud infrastructure with built-in redundancy

4.2 Storage Locations

- **Locations:** Backups are stored in geographically separated Azure regions. Customers have the choice of their data being stored either in the UK or EU with primary and secondary locations within each jurisdiction.
- **Primary Storage:** UK South or North Europe with automated backup capabilities:
- **Secondary Storage:** UK West or West Europe.

4.3 Retention Summary

- **Point-in-Time Restore:** 14 days (7 days for sandbox environments)
- **Weekly Backups:** 12 weeks retention
- **Monthly Backups:** 24 months retention
- **Yearly Backups:** 7 years retention

5. SECURITY AND ENCRYPTION

5.1 Data Protection

- All backups are encrypted both in transit and at rest using industry-standard encryption (AES-256)
- Access to backup systems is restricted to authorised personnel only
- Multi-factor authentication required for all backup system access
- Regular security audits and penetration testing of backup infrastructure

5.2 Data Integrity

- Backup integrity checks performed automatically with each backup operation
- Regular restoration testing to verify backup completeness and accuracy
- Checksums and hash verification for all backup files

6. RECOVERY TIME AND POINT OBJECTIVES

6.1 Service Level Targets

- **Recovery Time Objective (RTO):** 4 hours for critical systems restoration
- **Recovery Point Objective (RPO):** Maximum 1 hour of data loss for critical data
- **Backup Restoration Time:** Standard restoration requests processed within 24 hours

6.2 Priority Classifications

- **Critical Systems:** Customer-facing applications and databases
- **Important Systems:** Internal tools and non-critical customer features
- **Standard Systems:** Administrative and support systems

7. MONITORING AND TESTING

7.1 Backup Execution and Monitoring

- **Automated Backups:** All backups are automated using Azure's built-in backup capabilities
- **Continuous Monitoring:** Implemented to ensure backup integrity and detect any failures
- **Alerts and Notifications:** Automated alerts sent to the designated Platform team in the event of backup failures or issues
- **Real-time Monitoring:** Continuous oversight of backup operations and system health

7.2 Disaster Recovery Testing

- **Active Data-Replication Testing:** Regular verification of real-time replication to secondary Azure data centres

- **Quarterly Recovery Drills:** Comprehensive testing of backup restoration procedures
- **Annual Business Continuity Testing:** Full-scale disaster recovery scenario testing
- **Point-in-Time Restore Validation:** Regular testing of database restoration capabilities