SECURITY ARCHITECTURE & DATA GOVERNANCE OVERVIEW

2025|2026 Edition

Foreword

Welcome to iplicit. We provide innovative cloud accounting software solutions, designed as a "true cloud" product. This means we harness the power of Microsoft's renowned Azure platform to deliver our services directly to you.

With iplicit, you can access your financial information from anywhere with an internet connection, freeing you from the constraints and costs of traditional on-premises servers. Our software is built for ease of use, with intuitive navigation, and it's designed to grow alongside your business, adapting to your changing needs.

At the heart of everything we do is an unwavering commitment to the security and protection of your data. We employ robust measures, including advanced encryption, to safeguard your valuable information and ensure your data remains confidential and protected from unauthorized access. and automatic backups, to safeguard your valuable information.

Our goals are simple:

- To provide you with secure, reliable cloud accounting services you can depend on.
- To ensure your data is always protected and that we comply with all relevant regulations, including the General Data Protection Regulation (GDPR).
- To offer solutions that scale with your business, supporting your journey to success.
- To deliver an experience that is not just powerful, but genuinely user-friendly.
- To maintain the highest levels of service availability and reliability, so iplicit is there when you need it.

iplicit provides a modern, powerful, and secure cloud-native financial management solution designed to meet the complex needs of mid-market organisations. The transition to a cloud platform, especially for managing critical financial data, is a decision built on trust. This document provides a comprehensive and technically detailed overview of the iplicit security architecture, its operational controls, and its governance framework. It is intended to offer transparent, verifiable information for customers, partners, and their technical teams conducting due diligence, demonstrating an unwavering commitment to the highest standards of data protection, service reliability, and regulatory compliance.

The effectiveness of this document for both business decision-makers and technical architects hinges on clear communication. Business leaders require swift assurance of security and compliance, while technical reviewers demand deep, verifiable evidence of robust controls. By structuring the information to serve both needs, this document aims to be not just a technical specification but a strategic asset for building confidence. It acknowledges that security due diligence is a cornerstone of the business decision-making process.

The security posture of the iplicit platform is built upon three foundational pillars, which form the basis of this report:

1. **A Secure Foundation:** The platform is architected exclusively on Microsoft Azure, a leading global cloud provider. This strategic decision allows iplicit to leverage Microsoft's multi-billion-dollar investment in secure, resilient, and compliant global infrastructure, enabling the iplicit engineering team to focus on securing the application and data layers where it can add the most value.
2. **Secure by Design:** Security is not an ancillary feature but a core, non-negotiable requirement embedded in the platform's architecture and the entire software development lifecycle. From an architectural model that provides the strongest possible data isolation to a development process that proactively identifies and mitigates vulnerabilities, security is a foundational principle, not a final-stage inspection.
3. **Independently Verified Trust:** iplicit's commitment to security and quality is not merely a policy statement. It is validated through adherence to and certification against globally recognised standards, including ISO/IEC 27001. This framework of independent attestation provides external assurance that the controls and procedures detailed herein are part of a formal, audited, and managed system.

This document deconstructs each of these pillars, providing the necessary technical and procedural detail to validate iplicit's security claims. The ultimate goal is to demonstrate an unwavering commitment to being a trustworthy custodian of customer data, enabling organisations to modernise their financial operations with confidence.

Contents

Introduction

The integrity of the iplicit service is underpinned by a formalised framework of security and quality management, validated by internationally recognised standards and regulatory bodies. This framework establishes the foundation of trust upon which all technical controls and operational procedures are built.

iplicit is a UK-based company providing an advanced, cloud-native accounting software platform specifically engineered for the needs of mid-market organisations. The primary purpose of the solution is to offer a modern, flexible, and powerful financial management system for businesses and non-profit entities that have outgrown basic accounting packages or seek to migrate from outdated, on-premises legacy software. iplicit effectively bridges the gap between entry-level systems and the high cost and complexity of traditional Enterprise Resource Planning (ERP) systems.

The platform delivers sophisticated functionality, including multi-dimensional analysis and reporting, process automation, and seamless integration with other business applications via secure Application Programming Interfaces (APIs). Key value propositions include modernising financial operations by facilitating a smooth transition to a secure cloud environment, supporting organisational growth with a scalable platform, and offering a compelling, user-friendly alternative to established legacy software providers.

Key aspects of our purpose include:

- **Modernising your financial operations:** We help your organisation transition smoothly from traditional, often restrictive, accounting software to a more agile, accessible, and secure cloud environment.
- **Supporting your growth:** We provide a scalable platform that effortlessly accommodates the increasing complexity of your financial management as your business or non-profit expands.
- **Enhancing your reporting and analysis:** Our robust, real-time reporting tools offer multi-dimensional analysis, giving you deeper insights into your financial performance.
- **Streamlining your processes:** We automate financial tasks and workflows, improving your team's efficiency and reducing manual administration.
- **Facilitating seamless integration:** We enable easy connection with your other essential business systems, such as CRM, HR and payroll, through secure Application Programming Interfaces (APIs).

- **Serving specific sector needs:** Our software is tailored with functionalities relevant to various sectors, including non-profits (e.g., fund and grant management), education (multi-academy trusts, colleges), and other commercial enterprises.
- **Providing a UK-focused solution:** We develop and support our software with a keen understanding of the specific requirements of UK-based organisations.
- **Offering a better alternative:** We present a compelling choice compared with established legacy software providers and overly complex ERP systems, with a strong emphasis on ease of migration and use.

In essence, our purpose is to empower your mid-sized organisation with advanced, yet user-friendly and cost-effective, cloud accounting software that supports your growth and evolving financial management needs. This document details our security architecture, giving you a comprehensive view of our security practices and measures. As you will see, our architecture is designed with multiple layers of security, ensuring your data is protected, our service is reliable, and our operations maintain the highest integrity.

We aim to provide transparency and demonstrate our unwavering commitment to maintaining a secure environment for your data.

Certifications and Attestations

iplicit's commitment to security and quality is not merely a policy statement but is validated through adherence to and certification against globally recognised standards. A robust security program must be verifiable. For customers and their technical teams, independent, third-party attestations provide a critical baseline of credibility, confirming that a vendor's security and quality management systems are not just claimed but are designed, operated, and audited effectively against internationally recognized standards. iplicit's certifications represent a formal, managed system for protecting information, demonstrating a mature and systematic approach to security that underpins all technical controls.

iplicit holds the following active certifications and registrations, which affirm its commitment to security, quality, and regulatory adherence:

- **ISO/IEC 27001:2022 (Certificate No. 246393):** As the international gold standard for Information Security Management Systems (ISMS), this certification validates that iplicit has implemented a comprehensive and systematic framework of policies, procedures, and controls to manage information security risks. It is a testament to a mature, risk-based approach to security governance.
- **ISO 9001:2015 (Certificate No. 210103):** This standard for a Quality Management System (QMS) demonstrates iplicit's commitment to consistent quality and process excellence in its product development, service delivery, and customer support functions.
- **UK Information Commissioner's Office (ICO) Registration (No. ZA150166):** This registration confirms iplicit's formal commitment to complying with UK data protection laws, including the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).
- **Financial Conduct Authority (FCA) Registration (No. 07194134):** As a registered Account Information Service Provider (AISP), iplicit demonstrates adherence to the stringent regulatory requirements governing financial services in the United Kingdom, a critical credential for a financial management platform.

Beyond its own direct certifications, iplicit's security posture is significantly enhanced by its strategic choice to build exclusively on Microsoft Azure. Azure maintains the broadest compliance portfolio in the industry, with more than 100 offerings covering global, regional, and industry-specific requirements. This creates a powerful "halo effect," where the trust and compliance of the underlying platform extend to the iplicit application. While iplicit is responsible for the security *of* its application in the cloud, it inherits a foundation that is already certified for standards that customers in highly regulated industries may require, such as SOC 1/2/3, PCI DSS for financial data, and HIPAA for healthcare information. This strategic platform choice demonstrates foresight and proactively addresses a wide range of customer compliance needs, providing a secure and compliant foundation upon which the iplicit service is built.

Our foundation: leveraging Microsoft Azure

iplicit's security and reliability are fundamentally built upon Microsoft Azure. The platform is architected "exclusively on Microsoft Azure," allowing iplicit to leverage Microsoft's "multi-billion-dollar investment in secure, resilient, and compliant global infrastructure". This strategic decision, particularly the adoption of a 'Platform-as-a-Service (PaaS)-first' model, enables iplicit to focus its engineering and security resources on the application and data layers, where it can add the most value.

Azure maintains an extensive compliance portfolio, boasting over 100 offerings covering global, regional, and industry-specific requirements. This creates a powerful "halo effect," where the trust and compliance of the underlying platform extend to the iplicit application. While iplicit is responsible for the security of its application in the cloud, it inherits a foundation that is already certified for standards that customers in highly regulated industries may require, such as SOC 1/2/3, PCI DSS for financial data, and HIPAA for healthcare information.[1] This strategic platform choice demonstrates foresight and proactively addresses a wide range of customer compliance needs, providing a secure and compliant foundation upon which the iplicit service is built. This approach ensures that while Azure secures the cloud

infrastructure, iplicit secures *customer financial data and the application* within that cloud, implementing advanced controls such as database-per-tenant isolation and cryptographic erasure.

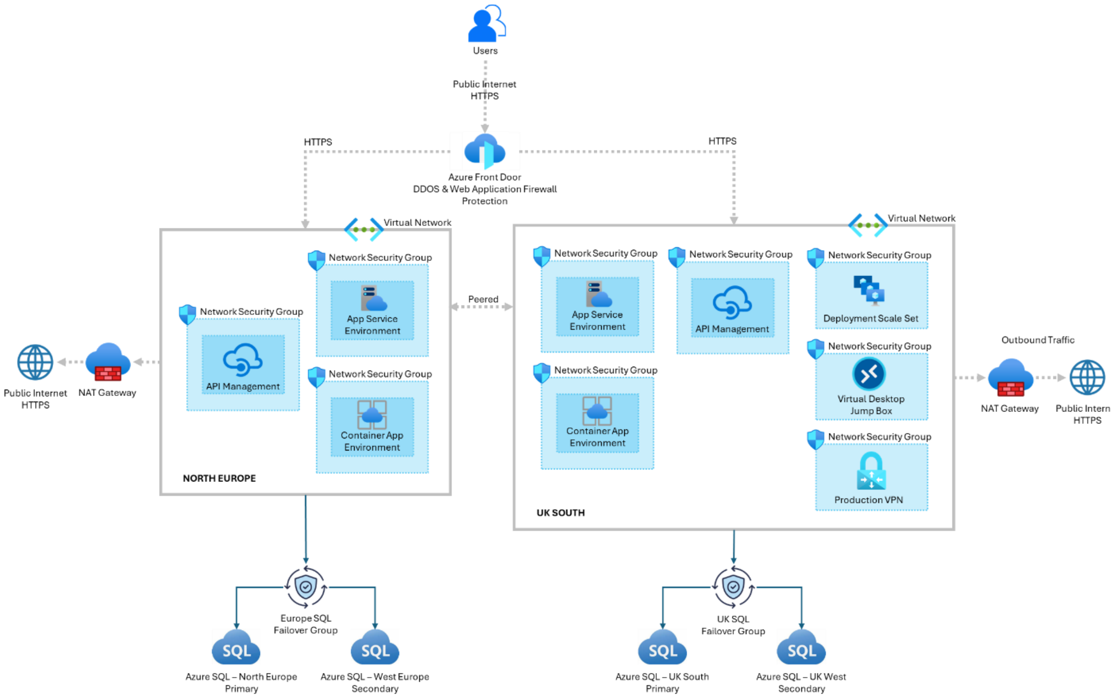

Diagram: iplicit architecture at high-level.

A Defence-in-Depth Approach

The iplicit security philosophy is rooted in the principle of "Defence-in-Depth," a multi-layered approach to security that assumes no single control is infallible. By implementing overlapping and complementary security controls across the entire technology stack, the platform is protected against a wide range of threats. This strategy ensures that if one layer of defence is bypassed, subsequent layers are in place to detect and prevent a breach.

The iplicit security architecture can be visualized as a series of concentric rings of protection, starting from the physical infrastructure and moving inward to the data itself:

- **Infrastructure Layer:** The foundation is the physically secure, resilient, and globally distributed Microsoft Azure infrastructure.
- **Network Layer:** This layer includes protections at the network edge, such as web application firewalls and DDoS mitigation, as well as internal network segmentation to isolate critical resources.
- **Application Layer:** Security is built directly into the iplicit application through a secure development lifecycle, robust authentication mechanisms, and granular access controls.
- **Data Layer:** At the very core, customer data is protected through strong architectural isolation, end-to-end encryption, and rigorous governance policies.

A fundamental concept in cloud security is the Shared Responsibility Model, which defines the division of security obligations between the cloud provider (Microsoft), the SaaS vendor (iplicit), and the customer. Clearly defining these boundaries is critical for establishing a strong security partnership and managing expectations. It clarifies the scope of each party's responsibilities, helping customers understand their role in the security ecosystem, such as managing their own user credentials and endpoint security. This transparency prevents misunderstandings and demonstrates that iplicit has holistically considered the entire security lifecycle.

The following table outlines this model as it applies to the iplicit service.

Responsibility Area	Microsoft Azure (The Cloud)	iplicit (In the Cloud)	Customer (Using the Cloud)
Physical Security	Secures datacentres, servers, and network hardware.	N/A	Secures their own physical offices and locations.

Infrastructure Security	Secures the hypervisor, network fabric, and underlying cloud infrastructure.	N/A	N/A
Platform Security	Manages and patches the operating systems and runtime environments for PaaS services (e.g., App Services, Azure SQL).	N/A	N/A
Application Security	N/A	Secures the iplicit application code, manages vulnerabilities, and validates security controls.	N/A
Data Security	Provides tools for encryption and isolation.	Implements data isolation (database-per-tenant), end-to-end encryption, key management, and secure deletion processes.	Responsible for the classification and appropriate handling of the data they enter into the system.
Identity & Access	Secures access to the Azure management plane.	Secures and audits its own personnel's privileged access to the production environment. Provides tools for customer access management.	Manages and secures their own user accounts, credentials, roles, and permissions within the iplicit application. Enforces their own password and MFA policies.
Endpoint Security	N/A	Secures and manages all corporate endpoints (laptops) used by its personnel to access iplicit systems.	Secures and manages all endpoints (desktops, laptops, mobile devices) used by their employees to access the iplicit service.

Governance & Compliance	Maintains compliance certifications for the Azure platform.	Maintains certifications for the iplicit service (e.g., ISO 27001) and ensures compliance with regulations like GDPR.	Responsible for using the iplicit service in a manner that complies with their own internal policies and industry regulations.

Resilient Infrastructure and Operations

The reliability and security of the iplicit service are built upon a foundation of resilient infrastructure and vigilant, continuous operational oversight. This section details the foundational security of the platform's architecture, and the operational processes designed to ensure stability, protect against attacks, and guarantee service availability and recoverability. It provides assurance that the platform is stable, reliable, and constantly monitored.

Core Infrastructure and Geo-Resilience

High availability and disaster recovery are architected into the platform through a multi-layered approach to geo-resilience. iplicit operates a multi-regional deployment strategy across paired Azure regions to ensure service continuity and data durability. The primary region pairs are:

- **United Kingdom:** UK South (London) paired with UK West (Cardiff)
- **Europe:** North Europe (Ireland) paired with West Europe (Netherlands)

This pairing ensures that data can be replicated to a separate geographical location, protecting against large-scale regional disasters.

Within each region, iplicit leverages **Azure Availability Zones (AZs)** to protect against datacentre-level failures. An AZ is a unique physical location within an Azure region, comprising one or more datacentres equipped with independent power, cooling, and networking. The physical separation between AZs is substantial enough to mitigate the impact of localised incidents, while they remain connected by a high-performance, low-latency network with a round-trip latency target of less than 2 milliseconds. This low latency is critical as it enables high-performance synchronous data replication between zones, a key component for achieving stringent recovery objectives.

iplicit's architecture utilises both of Azure's availability models to build a fault-tolerant system:

- **Zone-Redundant Services:** For many platform components, iplicit uses zone-redundant services where Azure automatically replicates data and distributes workloads across multiple AZs. In the event of a zone failure, Azure manages the failover transparently, ensuring service continuity.
- **Zonal Services:** For other components, such as virtual machines, iplicit employs a zonal deployment strategy. This involves proactively deploying multiple instances of a resource across different AZs and managing the replication and failover process to ensure resilience.

This combination of multi-region and multi-zone deployment creates a deeply resilient infrastructure capable of withstanding a wide range of failure scenarios, from individual component failures to entire datacentre or regional outages.

Edge Security and Network Architecture

To ensure performance and safety, all internet-facing traffic to the iplicit platform is managed and secured by a global security network that filters and inspects requests before they can reach the core application servers.

This is primarily achieved through **Azure Front Door**, which serves as a global, scalable, and secure entry point for all web traffic. Front Door provides several critical security functions:

- **DDoS Protection:** The platform benefits from Azure's built-in, platform-level protection against common network-layer (Layer 3/4) Distributed Denial of Service (DDoS) attacks. This infrastructure-level defense is designed to absorb and mitigate large-volume attacks at the network edge.
- **Web Application Firewall (WAF):** Integrated with Front Door is a powerful WAF that provides protection against application-layer (Layer 7) threats. iplicit utilizes the Premium tier of Front Door, which includes Microsoft-managed rule sets that are continuously updated to defend against common vulnerabilities outlined in the OWASP Top 10, such as SQL Injection (SQLi) and Cross-Site Scripting (XSS). This tier also provides advanced bot protection rules based on Microsoft's extensive threat intelligence data.
- **Intelligent Routing and Failover:** Front Door continuously monitors the health of iplicit's backend application instances across different regions. If an instance or an entire region becomes unhealthy, Front Door automatically and seamlessly routes traffic to the next available healthy backend, providing rapid failover and maintaining high availability for users.

The iplicit production environment resides within a secure Azure Virtual Network (VNet), which is a private, isolated network space in the cloud. This VNet is logically segregated from all other networks, such as those used for development and testing. This network isolation is enforced by multiple layers of controls:

- **Network Security Groups (NSGs):** These act as a distributed, stateful firewall, with rules configured based on the principle of least privilege to allow only necessary traffic between resources.
- **Azure Private Link:** This is used to secure connections to backend services, such as Azure SQL Databases. Private Link ensures that traffic between the application and the database travels over the Microsoft private backbone network, completely avoiding exposure to the public internet and forming a key component of a Zero Trust security model.

Data Protection and Governance

The protection and governance of customer data represent the most critical aspect of the iplicit security framework. A multi-layered strategy is employed to ensure data is logically isolated, encrypted end-to-end, and managed in strict accordance with regulatory requirements and privacy principles.

Multi-Tenant Data Isolation Architecture

A fundamental architectural decision in any multi-tenant SaaS application is the data isolation model. iplicit has deliberately implemented a database-per-tenant model, providing the highest possible degree of data isolation. In this architecture, each customer is provisioned with their own dedicated, logically separate Azure SQL Database. This approach offers significant security and operational advantages over alternative models, such as sharing a database and using tenant ID columns with Row-Level Security (RLS) to enforce separation. This single, fundamental choice is not an isolated feature but a strategic decision that has profound, compounding positive impacts across multiple security and operational domains.

The benefits of this chosen architecture are comprehensive:

- **Strongest Data Isolation:** There is no physical or logical path for one tenant's data to be accessed by another at the database layer. This directly leads to the strongest data isolation, eliminating any possibility of cross-tenant data leakage at the database layer.
- **Performance Isolation:** The "noisy neighbour" problem, where a heavy workload from one tenant can degrade performance for others in a shared database, is effectively mitigated. Resources can be managed on a per-tenant basis.
- **Simplified Operations:** Critical operations like tenant-specific backup, point-in-time restore, and data export become straightforward and low-risk.
- **Verifiable Data Deletion:** This model enables a clean, complete, and verifiable process for deleting a tenant's data upon contract termination. Dropping a dedicated database effectively removes the data without requiring complex row-level deletion logic.
- **Simplified Security Management:** It facilitates a centralized and robust security model, reducing the complexity of managing access controls compared to shared-schema approaches.
- **Compliance & Auditability:** It simplifies demonstrating data residency, isolation, and deletion processes to auditors and regulators.

The following table compares iplicit's chosen model against common alternatives, justifying the architectural decision based on key security and compliance criteria. This table is highly persuasive and a significant differentiator, moving beyond a mere statement of fact to a compelling, evidence-based justification for iplicit's strategic architectural choice. It directly addresses a core security concern with verifiable evidence and a clear comparison, demonstrating iplicit's foresight and commitment to the highest level of data isolation.

Feature	Database-per-Tenant (**iplicit's Model**)	Sharded Multi-Tenant Database	Shared Database (Single Schema with RLS)
Data Isolation	High. Data is physically and logically separated in its own database container. No possibility of cross-tenant queries at the database level.	Medium. Data for a single tenant is co-located with other tenants on a shard. Isolation relies on application logic and sharding key enforcement.	Low. All tenants' data resides in the same tables. Isolation is entirely dependent on application-level code (RLS), which carries a higher risk of misconfiguration or bypass.
Performance Isolation	High. The "noisy neighbour" effect is mitigated. Resources can be scaled on a per-tenant basis if required.	Medium. A noisy neighbour can impact other tenants on the same shard. Tenant-specific performance management is complex.	Low. A single tenant's heavy queries can consume shared resources and degrade performance for all other tenants in the database.
DR Complexity	Low. Restoring a single tenant is a simple, standard database restore operation that does not impact any other tenant.	Medium. Restoring a single tenant requires identifying the correct shard and performing a restore, which may affect other tenants on that shard.	High. Restoring a single tenant from a backup of a large, shared database is a complex and high-risk operation, often requiring a partial restore to a separate location and manual data extraction.
Secure Deletion Verifiability	High. Deleting the dedicated database is a complete and verifiable action. Backups expire naturally according to retention policies,	Medium. Deletion requires removing tenant-specific data from a shared shard, which is harder to verify completely.	Low. Deletion requires finding and removing specific rows from shared tables, leaving a higher risk of data

	ensuring no data remains indefinitely.		remnants. Verification is difficult.
Compliance & Auditability	High. The clear separation simplifies demonstrating data residency, isolation, and deletion to auditors and regulators.	Medium. Demonstrating isolation requires auditing both the database and the application logic.	Low. Demonstrating isolation is complex and relies heavily on code reviews and proving the infallibility of the RLS implementation.

Data Encryption Protocols

iplicit enforces robust encryption for all customer data, both when it is moving across networks (in transit) and when it is stored on disk (at rest). All external and internal communication with the iplicit platform is encrypted using Transport Layer Security (TLS) 1.3, the latest and most secure version of the protocol, offering significant cryptographic improvements. All public-facing TLS certificates are provided by a trusted Certificate Authority, DigiCert.

All customer data stored within the iplicit environment is encrypted at rest using the Advanced Encryption Standard (AES) with a 256-bit key (AES-256), a FIPS-validated, symmetric encryption algorithm recognized globally as the standard for securing sensitive and classified data. For data stored in Azure SQL Databases, this is implemented via Transparent Data Encryption (TDE), which performs real-time encryption and decryption of the database, its backups, and transaction log files at the page level. All customer file attachments stored in Azure Storage are also encrypted at rest using AES-256.

Cryptographic Key Management

The security of an encryption system fundamentally depends on the security of its cryptographic keys. iplicit employs a robust, centralized key management strategy using **Azure Key Vault**, a secure, hardware-backed service for managing cryptographic keys, secrets, and certificates.

Rather than managing keys within the application code where they might be exposed, iplicit offloads this critical function to Azure's dedicated key management infrastructure. This ensures that:

- **Secure Storage:** Encryption keys are stored in highly secure Hardware Security Modules (HSMs) or FIPS 140-2 validated software-protected vaults, separating the data from the keys used to protect it.

- **Strict Access Control:** Access to the Key Vault is strictly governed by Azure's modern Role-Based Access Control (RBAC) model, enforcing the principle of least privilege. Only authorized system processes and personnel with specific, audited roles can interact with the vaults.
- **Safety Mechanisms:** Key Vault's built-in data protection features, such as "soft-delete" and "purge protection," are fully enabled. This prevents the accidental or malicious deletion of keys, ensuring that data remains accessible and recoverable throughout its lifecycle.
- **Automated Rotation:** Policies for key rotation are implemented to limit the amount of data encrypted with a single key version, further reducing cryptographic risk.

Data Governance and Regulatory Compliance

iplicit maintains a comprehensive data governance program to ensure compliance with legal and regulatory obligations and to uphold its commitment to data privacy. The platform and its operational processes are designed to be fully compliant with the **General Data Protection Regulation (GDPR) 2016/679** and the **UK Data Protection Act 2018 (UK GDPR)**.

Data Residency and Sovereignty iplicit provides customers with a choice of data residency, ensuring all customer data—including primary database content, file attachments, and backups—is processed and stored exclusively within the customer's chosen geographical region (either the UK or the EU). Data is never moved outside of this region without explicit customer consent, ensuring data sovereignty requirements are met.

Sub-processor Management A rigorous due diligence process is conducted for all third-party sub-processors to ensure they meet iplicit's stringent security and privacy standards. All sub-processors are bound by Data Processing Agreements (DPAs) that enforce GDPR compliance. For any sub-processors located in the United States, iplicit ensures they are active members of the EU-U.S. Data Privacy Framework or bound by GDPR-compliant DPAs, providing a legal mechanism for secure data transfers.

Privacy by Design The principle of "privacy by design" is embedded in iplicit's development and change management processes. Before the implementation of any new project or system that processes personal data, a Data Protection Impact Assessment (DPIA) is conducted to systematically identify, analyse, and minimize data protection risks.

Managing Data Subject Rights iplicit supports customers in fulfilling their obligations under GDPR. As the data controller, the customer retains full control over the data they input into the system. Customers are responsible for using the application's standard editing and deletion features to rectify or remove specific personal data fields as required to comply with Data Subject Access Requests (DSARs) or the "Right to be Forgotten".

Data Retention and Secure Deletion Lifecycle

iplicit provides a clear, robust, and verifiable process for the secure deletion of customer data at the end of the service relationship. This process is directly enabled by the architectural decision to use a database-per-tenant model, ensuring that a customer's data can be isolated and removed without affecting others.

By default, iplicit retains customer data for the duration of the active service contract. Upon termination, data is retained for a defined period as specified in the service agreement. During this period, the customer retains the ability to export their data.

Data Export and Retrieval Customers are responsible for retrieving their data prior to the final deletion of their environment. This is achieved through the standard data export and reporting features provided within the iplicit application. iplicit does not provide customers with direct access to raw database backup files or underlying storage containers.

Deletion Process Once the post-termination retention period expires, or upon a verified request for deletion (subject to the terms of the service agreement), the data enters the secure deletion lifecycle. This is a multi-step procedure designed to ensure the removal of customer data from the production environment:

1. **Deletion of Live Data:** The tenant's live data stores are permanently deleted. The entire Azure SQL Database dedicated to the tenant is dropped, and the corresponding Azure Storage container holding all file attachments is permanently deleted. This removes all primary data and attachments from the live production systems.
2. **Backup Expiration:** Encrypted copies of the data will continue to exist within the geo-replicated backup cycle until they naturally expire. These backups are retained strictly according to the defined retention policy (e.g., 14 days for Point-in-Time Restore). Once the retention period for a specific backup file elapses, it is automatically and permanently overwritten by the Azure platform.
3. **Verification:** All deletion actions are logged internally to ensure traceability and adherence to the defined lifecycle policy.

Identity and Access Management (IAM)

A robust Identity and Access Management (IAM) framework is essential for ensuring that only authorized individuals can access the iplicit service and its underlying infrastructure. iplicit implements distinct and stringent IAM controls for both its customers and its own internal personnel.

Customer Authentication and Federation

iplicit provides flexible and secure authentication options, allowing customers to integrate the service seamlessly with their existing corporate identity infrastructure. The platform fully supports modern authentication standards, including SAML 2.0 and integration with Microsoft Entra ID (formerly Azure Active Directory), enabling Single Sign-On (SSO). This centralizes user authentication management and improves the user experience. Multi-Factor Authentication (MFA) is supported and strongly recommended, typically enforced by the customer's corporate identity provider. For customers not using SSO, iplicit enforces a robust default password policy as a minimum-security baseline.

Application-Level Access Control

Within the iplicit application itself, a granular authorization system ensures that authenticated users can only access the data and functionality relevant to their roles. iplicit features a comprehensive in-app Role-Based Access Control (RBAC) system, distinct from Azure RBAC, allowing customer administrators to define specific roles based on job functions. Each role can be assigned a granular set of permissions, rigorously enforcing the principle of least privilege. All significant user and system actions within the application are recorded in a detailed, immutable audit log, critical for security monitoring, compliance, and forensic investigation.

Privileged Access Management for iplicit Personnel

iplicit enforces extremely strict controls over its own personnel's access to the production environment, operating under a Zero Trust security model where access is never granted by default. All workstations used by iplicit engineers and support staff are centrally managed using Microsoft Intune to enforce security configurations, compliance policies, and endpoint protection. All user identities are managed in Microsoft Entra ID, providing a single, secure source for authentication and authorization.

Crucially, iplicit has eliminated the concept of standing administrative privileges to its production environment. Access is granted using Azure Privileged Identity Management (PIM), meaning an engineer requiring access must submit a request for a specific, privileged role for a limited time. This request may require manager approval and is fully audited. The privileges are automatically revoked when the time expires, drastically reducing the window of opportunity for credentials to be compromised or misused. All requests for privileged access, and indeed all access by iplicit personnel to internal systems, are enforced with MFA. Furthermore, Microsoft Entra Conditional Access policies are used to apply additional contextual controls, such as requiring access to originate from a compliant, managed device or a trusted network location. This layered approach ensures that access to sensitive production systems is tightly controlled, monitored, and auditable. These stringent internal controls directly protect customer data by severely limiting the window of opportunity for insider threats or compromised credentials, providing an additional layer of external assurance. By showcasing such stringent internal controls, iplicit builds a stronger case for being a "trustworthy custodian". It effectively communicates that iplicit practices what it preaches, extending its security commitment to its own operational environment, which is a powerful and reassuring message for customers undergoing due diligence.

Secure Software Development Lifecycle (SSDLC)

iplicit's commitment to security is not an afterthought but a "core, non-negotiable requirement embedded in the platform's architecture and the entire software development lifecycle". This "Shift Left" philosophy treats security as a proactive and continuous process, not a final-stage quality gate, aiming to identify and remediate potential vulnerabilities as early as possible, thereby reducing risk and the cost of remediation. This approach ensures that fewer vulnerabilities reach production, leading to faster delivery of inherently secure features, reduced operational risk, and a higher quality, more reliable product for customers.

Before any code is written, a formal threat modelling process is conducted to identify potential security threats, attack vectors, and vulnerabilities, allowing for appropriate security controls to be designed into the architecture from the outset. All developers adhere to OWASP Secure Coding Practices, including rigorous input validation, strong server-side authorization checks, and secure error handling. Source code repositories are protected by Role-Based Access Control (RBAC), with mandatory peer reviews for all code changes and continuous scanning for sensitive information.

Automated security testing is integrated directly into the Continuous Integration and Continuous Deployment (CI/CD) pipeline. Static Application Security Testing (SAST) tools scan new code for known vulnerability patterns, providing real-time feedback. Software Composition Analysis (SCA) identifies third-party and open-source libraries, checking them against databases of known vulnerabilities (CVEs) to manage software supply chain risk. Automated security gates are configured to fail builds and block pull requests if critical vulnerabilities are detected, preventing security issues from progressing to production.

Following development and automated testing, a rigorous validation phase is conducted by dedicated Quality Assurance (QA) and security teams. This includes functional, performance, usability, and regression testing, with explicit verification of security controls. Furthermore, iplicit engages independent, certified cybersecurity partners to conduct regular, formal penetration tests against the production application and its supporting infrastructure. These tests simulate real-world attacks, providing invaluable, independent validation of the platform's overall security posture and the effectiveness of the entire SSDLC.

Security Operations and Business Continuity

Maintaining a secure and reliable service requires continuous vigilance and a state of constant preparedness. iplicit's Security Operations and Business Continuity framework is designed to protect the live production environment, detect and respond to threats, and ensure the service remains resilient and recoverable.

Continuous Monitoring and Threat Detection

The iplicit production environment is monitored 24/7 using a suite of advanced, integrated Microsoft security services that provide deep visibility and intelligent threat detection. Microsoft Defender for Cloud serves as the central hub for cloud security management, providing Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP). This service continuously assesses all Azure resources against security best practices, identifies misconfigurations, and provides actionable recommendations. It also offers workload-specific threat detection, including vulnerability assessments for servers and anomalous activity detection in Azure SQL Databases.

iplicit uses Microsoft Sentinel as its cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. Sentinel ingests and correlates security logs and alerts from all sources, using advanced analytics, machine learning, and User and Entity Behaviour Analytics (UEBA) to detect sophisticated threats. As a SOAR, Sentinel automates responses to common threats using "playbooks," enabling faster response times and reducing the burden on security analysts.

Vulnerability and Patch Management

A timely and effective vulnerability and patch management process is critical to protecting against known exploits. Under the cloud's shared responsibility model, Microsoft is responsible for patching the underlying PaaS infrastructure, while iplicit is responsible for identifying and patching vulnerabilities within its own application code and any third-party libraries or components it uses.

iplicit follows a structured process for managing vulnerabilities: Identification (through scans, SCA tools, and penetration tests), Prioritization (based on severity, business impact, and exploitability), and Remediation. iplicit is committed to remediating identified vulnerabilities in a timely manner, with a formal Service Level Agreement (SLA) in place that strives to address all critical and high-risk vulnerabilities in less than 14 days from confirmation.

Business Continuity and Disaster Recovery (BCDR)

iplicit maintains a comprehensive BCDR plan to ensure the service can be recovered swiftly and data integrity maintained in the event of a major disruption. The BCDR plan is built around formally defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets, with a target service availability of 99.8%.

The foundation of the recovery plan is a robust, automated, and geo-replicated backup strategy for all customer databases, ensuring multiple recovery points are available. The following table provides critical transparency and assurance regarding data recoverability and long-term data management, directly addressing fundamental customer concerns about data loss, business continuity, and data retention for compliance purposes.

Backup Type	Frequency	Retention Period	Purpose
Point-in-Time Restore (PITR)	Continuous	14 Days	Provides granular recovery to any point in time within the last two weeks, enabling rapid recovery from data corruption or accidental deletion with a very low RPO.
Weekly Full Backup	Weekly	12 Weeks	Provides a weekly recovery point for medium-term data restoration needs.
Monthly Full Backup	Monthly	24 Months	Serves as a monthly snapshot for longer-term archival and compliance requirements.
Yearly Full Backup	Annually	7 Years (extendable to 10)	Fulfils long-term data archival and regulatory retention obligations.

The Disaster Recovery (DR) plan leverages the multi-region Azure architecture. In the event of a catastrophic failure of an entire Azure region, iplicit will initiate a failover to the paired region, involving redirecting traffic via Azure Front Door and restoring the service and customer databases from the most recent geo-replicated backups. The entire DR plan is tested regularly to validate its effectiveness and ensure the RTO and RPO targets can be met.

Major Incident Management Framework

For high-impact service disruptions that do not trigger a full disaster recovery, iplicit follows a structured Major Incident Management (MIM) process designed for rapid resolution and clear communication. This framework demonstrates a mature, customer-centric approach to managing crises. Incidents are formally classified based on their impact on customers, which determines the urgency and resource allocation for the response. A major incident declaration triggers the immediate mobilization of a dedicated incident management team, with the primary objective of swift service restoration. Throughout the incident, iplicit is committed to providing clear, timely, and empathetic communication to all affected customers and partners. After every major incident is resolved, a formal Post-Incident Review (PIR) or Root Cause Analysis (RCA) is conducted to understand the causes and identify preventative measures.

The following matrix is highly effective in demonstrating a mature, customer-centric approach to incident management by setting clear expectations for communication and response during critical service disruptions, which is paramount for customer confidence during times of crisis. It builds trust by demonstrating iplicit's proactivity and preparedness in crisis management.

Priority Level	Definition/Business Impact	Example	Target Initial Response	Communication Cadence
P1 (Critical)	Complete service unavailability or critical functionality failure for a significant number of customers. Major business impact or data integrity concerns.	The entire iplicit application is inaccessible. Widespread inability to process financial transactions.	< 1 hour	Regular updates every 30-60 minutes or as new information is available.
P2 (High)	Significant service degradation or failure of a non-	A specific reporting module is failing for	< 4 business hours	Updates provided every 2-4 hours or

	critical but important feature for a group of customers. Moderate business impact.	multiple customers. Performance is severely degraded for a subset of users.		upon significant progress.

These operational details go beyond mere technical controls; they demonstrate a high degree of organizational maturity, preparedness, and accountability in managing the live production environment. A mature operational posture means that even when security incidents or service disruptions inevitably occur, iplicit has the established processes, advanced tools, and committed personnel to detect, respond, and recover quickly and transparently. This proactive (monitoring, patching) and reactive (BCDR, MIM) capability directly translates to higher service reliability, reduced downtime, and mitigated business risk for the customer. For customers, especially those migrating critical financial data, operational resilience and a clear, communicated incident response plan are as important as preventative security measures. The document effectively communicates that iplicit is prepared for both "if" and "when" scenarios, which is a significant trust builder during due diligence.

Our Commitment to Supply Chain Security

The security and integrity of the iplicit platform are fundamentally linked to the security of its supply chain. iplicit's Third-Party Risk Management (TPRM) program is an integral and mandatory component of its ISO/IEC 27001:2022 certified Information Security Management System (ISMS). A formal, risk-based methodology ensures that the level of scrutiny applied to any supplier is directly proportional to the risk they present to iplicit and its customers. This program is aligned with globally recognized standards, including the NIST Cybersecurity Framework, to ensure a comprehensive and defensible security posture.

Every potential vendor undergoes a formal Inherent Risk Assessment before engagement, evaluating them based on data sensitivity and service criticality. Suppliers are classified into two tiers:

- **Tier 1 (Key Suppliers):** Strategic partners integral to the iplicit platform or handling customer data. These high-risk vendors are managed through Risk Ledger, a collaborative supply chain security platform that provides continuous, near real-time visibility into their security posture. The use of Risk Ledger highlights a modern, transparent, and collaborative approach to supply chain security, differentiating iplicit from companies using less sophisticated, static assessment methods.

- **Tier 2 (Supporting SaaS Services):** Vendors providing essential business support functions that do not process customer production data. These undergo a thorough, evidence-based manual due diligence process, including meticulous review of SOC 2 Type II reports and ISO 27001 certificates/Statement of Applicability (SoA).

Supplier oversight is an ongoing process. Tier 1 suppliers are continuously monitored through Risk Ledger, while Tier 2 suppliers undergo formal re-assessment periodically. All supplier relationships are governed by legally binding contracts that include robust security clauses, comprehensive Data Processing Agreements (DPAs), strict SLAs for security breach notification, and a right to audit security controls.

iplicit maintains a formal, documented process for securely terminating any vendor relationship. This decommissioning protocol ensures that all forms of access are systematically and immediately revoked, and contractual clauses enforce the secure return or certified, permanent destruction of all iplicit data from the vendor's environment.

In today's interconnected SaaS ecosystem, a company's overall security posture is fundamentally linked to the security of its third-party suppliers and partners. By demonstrating a comprehensive and mature TPRM program, iplicit proactively addresses a major, often overlooked, external attack vector. This extends the circle of trust beyond iplicit's direct operational controls to its entire ecosystem of dependencies, directly mitigating a significant source of external risk for the customer's data. This section is crucial for sophisticated customers and technical architects who understand the growing threat of supply chain attacks. Its inclusion and detailed explanation demonstrate iplicit's comprehensive risk awareness and management, further solidifying its position as a truly secure and trustworthy partner.

Responsible Technology Innovation

iplicit is committed to leveraging new technologies to enhance the customer experience, improve efficiency, and deliver greater value. This innovation is always pursued responsibly, with security, ethics, and data privacy as foundational principles.

Use of Artificial Intelligence

As iplicit explores the potential of Artificial Intelligence (AI) to make its software smarter and more helpful, its approach is guided by a strict ethical and security framework. Core principles include:

- **Purposeful Innovation:** AI features are developed to solve real-world customer challenges and provide tangible benefits.
- **Ethical Foundation:** All AI initiatives are built on a framework of fairness, transparency, and accountability, designing AI to augment human capabilities.
- **Trust and Transparency:** iplicit is committed to being clear about how AI is used within its services.

The trust customers place in iplicit to protect their data extends fully to any use of AI. Any customer data used for AI purposes, such as training machine learning models, is handled on a consent-first basis and with the strictest adherence to data privacy regulations, including GDPR. AI features are developed with the same rigorous security standards and controls as the rest of the platform, leveraging Azure's secure infrastructure for all data processing. Where appropriate for model development, techniques such as data anonymization and aggregation are used to protect privacy. iplicit is dedicated to developing AI systems that are accurate, reliable, and fair, involving rigorous testing and validation to check performance and proactive efforts to identify and mitigate potential biases in data or models.

This section demonstrates a proactive and responsible approach to leveraging new technologies. By proactively outlining its ethical and security framework for AI, iplicit demonstrates foresight and a deep commitment to responsible innovation. This pre-empts future customer concerns about how their data might be used in AI contexts and builds trust not just for current services, but for future developments. It positions iplicit as a forward-thinking yet responsible partner, contributing to long-term customer confidence by showing that iplicit considers the broader societal and ethical implications of technology.

In Summary

The iplicit security architecture is a comprehensive, multi-layered framework designed to protect customer data and ensure service reliability at every level. By strategically building on the secure foundation of Microsoft Azure, iplicit leverages a PaaS-first philosophy that combines the scale and resilience of a global cloud leader with its own focused expertise in application and data security.

The architectural choice of a database-per-tenant model provides the strongest possible isolation for customer data, a decision that has positive cascading effects on performance, disaster recovery, and the verifiability of secure data deletion. This is complemented by end-to-end encryption using modern protocols like TLS 1.3 and AES-256, with cryptographic keys securely managed in a centralized, hardware-backed model within Azure Key Vault.

Security is not a reactive measure but is proactively embedded throughout the Secure Software Development Lifecycle. From threat modelling and secure coding standards to automated security scanning in the CI/CD pipeline and independent penetration testing, security is a continuous and integral part of the development process. This is supported by vigilant 24/7 security operations, leveraging advanced threat detection and response capabilities from Microsoft Defender for Cloud and Microsoft Sentinel.

Finally, a mature governance framework, evidenced by ISO 27001 certification and adherence to GDPR, ensures that all technical controls are supported by robust policies and procedures. Combined with a comprehensive Business Continuity and Disaster Recovery plan, this demonstrates iplicit's deep and unwavering commitment to providing a secure, compliant, and trustworthy financial management platform.

Contact

In the interest of precision and operational efficiency, iplicit maintains dedicated communication channels for specific functions. This ensures that all enquiries are managed by the personnel best equipped to provide a timely and accurate response. The matrix below outlines the appropriate channel for various types of enquiry.

Purpose of Enquiry	**Contact Details & Context**
Registered Office	1st Floor at Bobby's, The Square, 2-12 Commercial Road, Bournemouth, BH2 5LP
General & Sales Enquiries	Email: info@iplicit.com Telephone: 020 7729 3260
Information Security	Email: infosec@iplicit.com
Data Privacy & GDPR Enquiries	Email: datacompliance@iplicit.com