IFS Cloud Security

At IFS, cloud service security is managed through our Information Security Management System. Certified to the requirements of ISO 27001:2013, the system therefore aligns with international best practice. Our security controls are maintained in accordance with ISAE3402/SSAE18 SOC 1 and ISAE3000 SOC 2 compliance.

IFS Cloud Services leverage the Microsoft Azure cloud. Trusted by 95% of Fortune 500 companies, Microsoft Azure is a robust, market-leading public cloud platform offering enterprise grade services. We take care of all cloud-based elements 24 hours a day, 365 days a year: cloud infrastructure, server operating systems, databases, middleware and IFS software.

Azure's security compliance, geo-redundant storage, global data center infrastructure, and seamless integration with companies' existing IT assets and IFS software make Azure the perfect choice for our Cloud Services.

In this fact sheet, we provide an overview of IFS Cloud Security and you can find more in the IFS Service controls documents, available for our products and services on our Trust Center.

Key facts

At IFS, we apply best practice to:

- **Asset management**–through dedicated, specialist teams
- **Data encryption**–with sophisticated protection of data in transit and at rest
- **Physical security**–through modern, secure data centers
- **Backup and recovery**–via robust and resilient policies and crisis management processes
- **Malware protection**–with extensive, proactive tools and techniques
- **Communications security**–through sophisticated authentication and encryption
- **Security testing**– via frequent vulnerability scanning and penetration testing

Asset management

At IFS, asset management is split into four areas of responsibility:

- **Physical infrastructure:** The Microsoft Cloud Infrastructure and Operations (MCIO) team manages the physical infrastructure and data center facilities for all Microsoft online services. This includes both the physical and environmental controls within the data centers as well as the outer perimeter network devices (e.g. edge routers). The MCIO have no direct interaction with the Azure services themselves.
- **The Azure service:** Microsoft Service management and service teams, separate to the MCIO, manage the support of the Azure service itself. Made up of numerous teams, each is responsible for a specific aspect of the service and has engineers available 24x7 to investigate and resolve failures in the service. Segregation of duty principles are applied, and service teams do not, by default, have physical access to the hardware environments that make up Azure.
- **Azure IT assets:** These are provided as part of IFS Cloud Services and are managed by the IFS Cloud team. We hold an inventory of all such assets in a Configuration Management Database (CMDB). Such assets are only managed by the relevant IFS personnel who are responsible for their establishment, operational monitoring and maintenance and disposal at their end of life.
- **Customer data:** Data held within both the production and test applications are owned by, and the responsibility of, the IFS Cloud customer. Our customers are responsible for managing their data in accordance with its classification and handling requirements determined by any applicable laws or regulations and for complying with the terms of the applicable contract with us and any associated data processing terms.

Data encryption

Cryptography is used within the IFS Cloud Service to protect information both in transit and at rest. For data in transit, TLS encryption over HTTPS is employed, utilising a security certificate issued by a trusted authority to provide 2048-bit RSA public key encryption. We employ Certificate Authorities to allocate encryption keys rather than using self-signed certificates and give customers choice regarding who manages the keys, including the customer themselves.

Server-side encryption of data at rest is used for disk storage within the Azure based service, along with service-managed keys to securely handle encryption. Disk encryption protects both operating system disks and data disks with full volume encryption. Encryption keys and secrets are safeguarded in the Azure Key Vault.

Physical security

Customer data is stored within Microsoft Azure data centers. We chose Microsoft as our provider due to the company's strong commitment to security. For example, it invests more than USD 1 billion annually on cybersecurity R&D and complies with a broad range of international and industry standards, including ISO 27001, FedRAMP, SOC 1 and SOC 2. And with a team of more than 3,500 security experts and more certifications than any other cloud vendor, it's perfectly placed to securely store our customers' data.

Azure data centers have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building and on the data center floor. More information can be found at the Microsoft Trust Center and in the IFS Information Security Management document.

Backup and recovery procedures

At IFS, we operate a formal backup/recovery policy. Rest assured we will always:

- Store backups at a secondary Azure site. This protects you against ransomware attacks, as cybercriminals are unable to seize complete control of your data.
- Test restoration processes regularly. In addition to ensuring that our backup/recovery processes work effectively, we refresh customer test environments from live production environments, all in the Cloud, and which are then used to validate changes to production systems prior to deployment.

We've implemented comprehensive disaster recovery and crisis management processes for IFS Cloud Services. And to validate their effectiveness in recovering our services, we test them at regular intervals. In the event of a significant disaster, where an entire Microsoft Azure data center becomes unavailable, the service would be re-established at the secondary site Azure location and we would collaborate with the customer and support them in getting connected again as quickly as possible.

Malware protection

To fully secure our customers' data, we've deployed enterprise-grade anti-virus and malware protection services. We regularly patch the operating systems and infrastructure components that make up the service to keep them up to date and protected against the latest threats.

To minimize the possibility of disruption to our customers' business, any patching involving system down time is performed in consultation with the customer each time.

Communications security

Being hosted in Microsoft Azure, customers access the IFS Cloud Service via the internet using TLS encryption over HTTPS. Being segregated from their own on-premise IT environment, and traffic to and from the service being restricted to only the necessary protocols, provides customers additional protection against ransomware. In such an event, IFS will work with the customer to help maintain access to their service while they remediate any effects of malware on their local IT domain.

In order to implement, monitor, manage and maintain a customer's instance of IFS Cloud Services, we connect to it using a dedicated service, SupportNet. Using the industry standard Internet Protocol Security (IPsec), SupportNet keeps customer information secure by authenticating and encrypting data in transit through a VPN.

Security testing

We perform security testing at multiple stages during the development of an IFS Cloud Services instance. What's more, our R&D team collaborate with third party specialists to conduct extensive security testing throughout the development lifecycle of IFS products themselves. We check for security risks using industry best practice security frameworks, such as OWASP.

Penetration testing of IFS Cloud Services systems is performed by a trusted third-party partner, taking place annually or following any substantial change to the environment or solution components. Both infrastructure and application testing are included and testing is conducted from the internet to replicate real world use cases.