PUBLIC

IFS Information Security - IFS Customerville Service Controls

IFS Global ISMS

Date:	13/05/2022
Revision:	1
Owner:	Todd Williams
Approved By:	Richard Rogers

Contents

1. IFS Customerville Security Management

Cloud Security

Customerville uses Microsoft Azure to provide services for all systems and applications. Azure leads among other cloud competitors on security, privacy, and compliance. Microsoft Azure meets several industry specific compliance standards such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2. Security is embedded in Azure with industry-leading technologies and practices. Azure provides easy methods to log all resources and feed those into Azure Security Center to alert and report on incidents. The Customerville IT Ops team utilizes these tools within Azure to internally monitor and tracks all issues 24x7x365.

Data Security

Your data is important not only to you, but us as well. Customerville uses industry standards and best practices to protect your data. Our systems are hardened using industry best practices and recommendations (NIST and ISO). All feedback information is collected over TLS then encrypted at rest. Our applications provide role-based access (RBAC), IP restrictions, Geo-location restrictions, single sign on (SSO) capability, and data segregation. We also provide granular configuration settings to further refine security. Although your data may reside in shared infrastructure it is logically separated from other clients. If your own compliance requires it, we can also provide private single tenant systems.

Application Security

When it comes to our feedback system, our developers follow industry best practices during the software development lifecycle. Test, staging, production, and demo environments are completely separated. Production information is never used in any environment but protection, no sample data sent over to test or demo. Our web-based surveys and dashboards are scanned for vulnerabilities and mitigated regularly.

Monitoring

All systems, applications, dashboards, and surveys are monitored externally and internally with staff available on call 24x7x365. This includes monitoring for availability, vulnerabilities, malicious activity, threats, and performance metrics. Regular vulnerability scanning is conducted on virtual machines, applications, database servers, and other systems.

Plugging the holes

Our applications and systems are regularly scanned for vulnerabilities using technology that is constantly updated. Each vulnerability is tracked and remediated by our IT Ops team. Our systems and applications also go through annual risk assessments to help cover a broad range of issues. In addition, clients can request penetration tests of their surveys and dashboards. These are conducted per client as the information and practices are unique per client. We don’t want to miss something, so we look for the holes in our own fences before someone else finds them.

Compliance

We aim to make compliance transparent and easy for our clients by managing your information responsibly. Our security controls were audited and found to be compliant through a SOC II type 2 in 2017 and again with a SOC 2 Type 1 in 2019. These reports are available on request.

GDPR

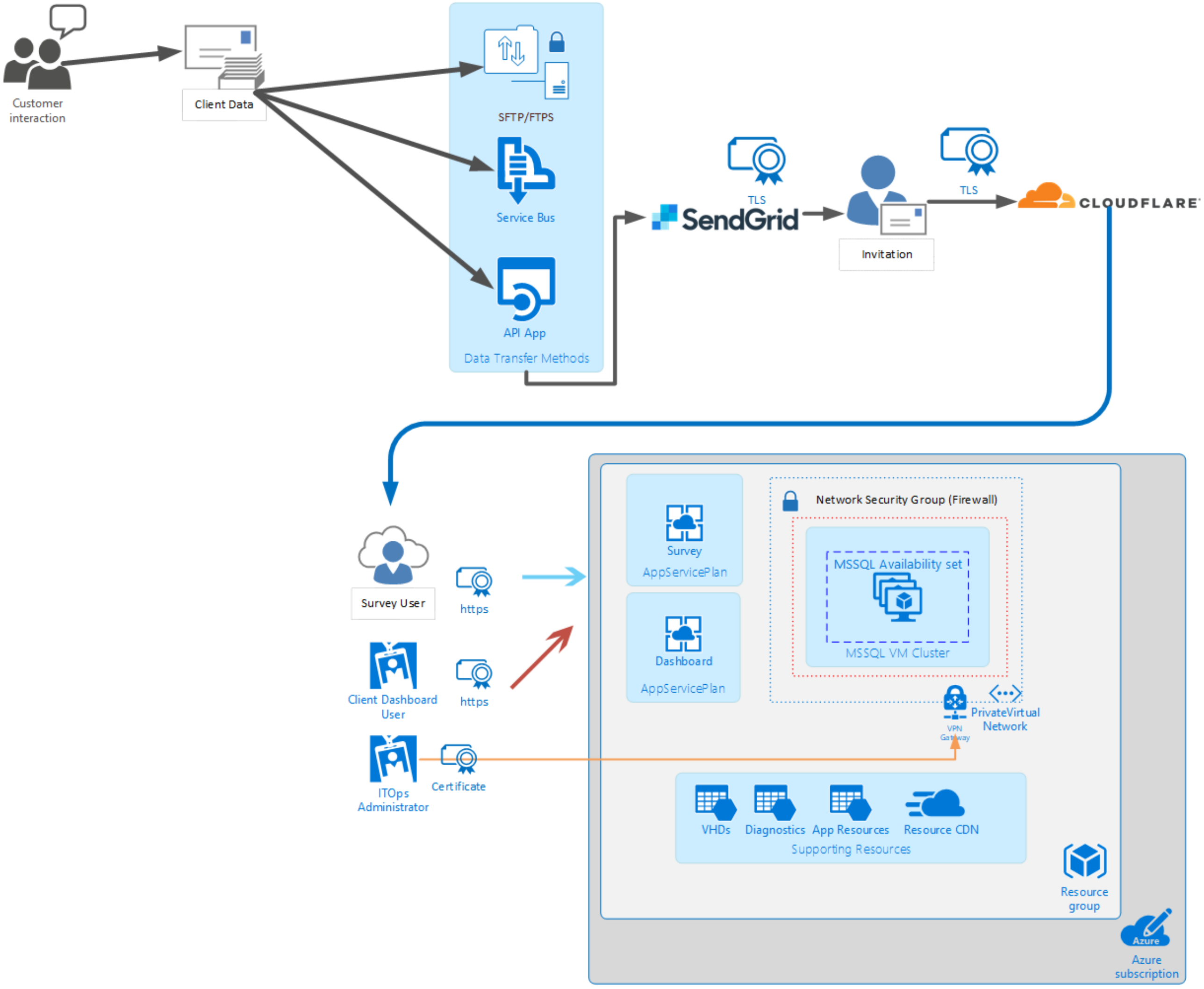
We believe GDPR brings strong privacy protection for our client's customers and want to provide that as a standard to all. Clients, employees, and client customers can correct, export, and/or permanently erase any personal information related to feedback Customerville has collected. More information can be found in our privacy policy. https://www.customerville.com/en/privacy

CCPA

To be honest, you don’t have to reside in California to request your information. The information provided in a survey by a respondent is their information. If they would like to see what we have collected, object to it, remove consent, erase it, or feel they were discriminated against we’re happy to comply. Customerville only collects information that is requested by our clients with consent of the respondent, we do not collect information ourselves. We never have and never will sell respondent information to third parties, and we don’t use that information for marketing. More information can be found in our privacy policy https://www.customerville.com/en/privacy

2. IFS Customerville Security Architecture

Customerville is deployed to Azure using geographic regions suited to our client's location. Regions are configured in subscriptions and are multi-tenant with logical separation of tenant data. Development, staging, and production environments are separated from each other.



3. Asset management

3.1. IT Assets

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 themselves have no direct interaction with the Azure services themselves.

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 24 x 7 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.

The Azure IT assets provided as part of the IFS Customerville Services are managed by the IFS Customerville IT Operations Team (ITOps). An inventory of all such assets is documented and maintained in the Azure portal. Such assets are only managed by the relevant IFS Customerville personnel who are responsible for their establishment, operational monitoring and maintenance and disposal at their end of life.

Customer onboarding comprises the establishment of the Azure virtualised services that host the specific IFS Customerville solution. This is followed by the installation of software assets onto the virtualised services then followed by the establishment of the secure customer connection in accordance with the connection method agreed with the customer (e.g. virtual network, private leased line, etc).

During the life of the IFS Customerville solution, the IFS Customerville IT Ops team are responsible for the monitoring and maintenance of the IFS IT assets, including the deployment of changes to the service in response to events such as software updates, security patches and service enhancements/extensions. All such changes are performed under formal change management utilising IFS' IT Service Management tools.

At the end of life of the IFS Customerville solution, all deployed IT assets are securely destroyed using the Azure administrative processes provided by Microsoft Azure and which are certified in accordance with ISO 27001 (as well as other internationally recognised security standards (please see Microsoft's Trust Center for more details).

3.2. Information Assets

IFS Customerville Information assets fall into one of two categories:

- Customer data
- IFS Customerville Service operations data

Processes and responsibilities for managing each of the above data categories are different and are described in the following sections.

Customer Data

Data held within both the production and test applications described in section 3.1 are owned and are the responsibility of the IFS Customerville customer. In execution of the IFS Customerville Services agreement, it is necessary for IFS to process information within these environments, for example when investigating a reported software issue. IFS has implemented procedures designed to ensure that customer data is processed only as instructed by the customer, throughout the entire chain of processing activities performed by IFS and its sub-processors. IFS has entered into written agreements with its sub-processors regarding privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. The document "List of IFS Sub-processors" sets out the current list of sub-processors involved with the delivery of IFS services including IFS Customerville.

IFS 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 IFS and any associated data processing terms.

Client data retention policy

- Within one business day of client termination all active surveys will be stopped and removed to prevent new data from being collected.
- Upon client termination and on client request a dump of all data can be made available to the client for download through secure FTP.
- Flat file dumps available through secure FTP will be maintained by Customerville for 90 days after contract termination. After 90 days the data will be destroyed.
- After 90 days from contract termination all client data will be removed from Customerville systems including the dashboard, databases.
- After 30 days of contract termination access to the dashboard for the client and client users will be removed.

At the point of termination of the IFS Customerville Services agreement, return and deletion of customer data will be in accordance with the terms of the agreement between IFS and the Customer.

IFS Customerville Service Operations Data

IFS Customerville Service operations data comprises the information associated with the management and operational delivery of the IFS Customerville Services itself for an individual customer. Such data comprises information such as system logs, system configuration files, error dumps etc. All such data is owned and managed by IFS and, with the exceptions of agreed service reporting and other data required to meet any applicable regulatory requirements, is not shared with third parties.

Upon termination of an IFS Customerville Services agreement, all such operations data will be deleted in accordance with the processes used to delete customer data described in the previous section and will therefore not be available post termination/expiration.

4. Access Control

The IFS Customerville Services includes a number of security controls which are used to restrict and protect access to both the IT and information assets that make up the service. Access controls are layered in accordance with the service layers that make up IFS Customerville solutions.

4.1. Microsoft Access to IFS Customerville Services

Employees (and contractors) of Microsoft involved with the delivery of Azure services have their employee status categorised with a sensitivity level that defines their access to Azure hosted services and data utilised as part of the IFS Customerville Services. A list of these role based access permissions can be found on the Azure Trust Center website and include roles ranging from Data Center Engineer with no access to Azure customer data up to Live Site Engineers who require access to Azure customer data in order to diagnose and mitigate platform health issues using diagnostic tools. All such users have a unique identifier to authenticate onto all assets and devices that make up the Azure environment.

Microsoft’s Azure operations personnel are required to use secure admin workstations (SAWs). With SAWs, administrative personnel use an individually assigned administrative account that is separate from the user's standard user account. The SAW builds on that account separation practice by providing a trustworthy workstation for those sensitive accounts.

4.2. IFS Administrative Access

As part of creating, managing and monitoring the IFS Customerville Services, IFS require the use of administrative level accounts which provide access to the Azure services and platforms that underpin the application solutions. These IFS controlled accounts are only made available to IFS personnel actively involved in the provision of the IFS Customerville Services and are allocated on an “as required” basis in accordance with the user’s job function, much like the principles applied by Microsoft and described in the previous section. These accounts comprise both Microsoft Azure accounts as well as administration accounts for the various infrastructure components that make up the particular IFS Customerville Service. Owing to the elevated permissions that the Azure accounts provide, multi-factor authentication is enabled to serve as an additional identity validation measure.

Access to the Microsoft Azure platforms and infrastructure that make up the IFS Customerville Service is not granted to IFS Customers.

4.3. Customer Controlled Application Access

Access to IFS Customerville Services requires authentication via one of the supported mechanisms described in the IFS Customerville Service Description (e.g. single sign-on using the customer’s existing Active Directory). All application level access is managed by the IFS customer, including user accounts provided to IFS in order to execute the services defined within the customer’s agreement with IFS (e.g. implementation services, support services, etc). Policies for such accounts are managed in accordance with the customer’s own access and identity policies (e.g. password policy enforced by the customer’s own Active Directory) subject to any technical constraints imposed by the IFS Customerville Service. The IFS customer can enable and disable such accounts using application administrator accounts provided to them as part of the IFS Customerville Service. It should be recognised that disabling accounts allocated to IFS may prevent delivery of the contracted services or fulfilling any applicable service level agreements.

4.4. Monitoring and Threat Detection

IFS Customerville Services are monitored for unauthorized intrusions using a combination of network and host-based intrusion detection mechanisms. IFS Customerville utilises threat protection facilities including continuous discovery and monitoring of Azure deployed resources and an assessment of their security status and any applicable security vulnerabilities that need remediation. Security alerts are sent to ITOps and tracked through an internal ticketing system.

IFS Customerville ITOps utilise monitoring and detection tools as part of their own service monitoring and which are supplemented by further security and health monitoring tools at the application level. External monitors are used for health monitoring. Alerts are sent to ITOps and tracked as tickets. Events requiring immediate attention are sent to staff on call.

4.5. Data Segregation

As shown earlier in this document, the production environment is held separately from the test and demonstration environments in Azure, enabling the deployment of system changes to be properly validated in a secure, safe test environment prior to deployment to production. All IFS development and support environments are also separated from the customer’s production environment with formal release management processes used to deploy system enhancements and corrections between environments.

5. Cryptography

Cryptography is used within the IFS Customerville Services to help protect information both in transit and at rest.

5.1. Encryption in Transit

All connectivity to the IFS Customerville Services over the public internet, used for the establishment of the services by the IFS Customerville IT Ops team, includes the use of RSA 2048-bit key encryption using TLS over HTPS. TLS provides strong authentication, message privacy and integrity (enabling detection of message tampering, interception and forgery), interoperability and ease of deployment and use. Perfect Forward Secrecy (FPS) protects connections between IFS' client systems and Azure cloud services by unique keys. SMB 3.0 is used by Virtual Machines running in Azure, ensuring data transfers are encrypted across Azure Virtual Networks.

IFS Customerville services are optionally configured to connect to customer IT domains using an Azure Virtual Private Network (VPN) gateway or ExpressRoute circuit. VPNs create a secure, encrypted tunnel (with the public internet as the underlying transport provider) to protect the privacy of data being sent into and out of Azure. Point to site VPN connections are used over SSTP (SSL) tunnels. A certificate from an internally managed CA is provided to each employee who has approved access. Authentication to devices on the virtual network behind the gateway require additional authentication using Azure AD credentials.

Azure Key Vault is used to safeguard cryptographic keys and secrets that cloud applications and services use. Permissions to access keys are restricted to authorised users and services only.

5.2. Encryption at Rest

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

Where Azure SQL Database is utilised as part of the IFS Customerville Services, server-side Transparent Data Encryption (TDE) is used via the Always Encrypted feature. TDE encrypts data files in real time, using a Database Encryption Key (DEK), which is stored in the database boot record for availability during recovery. TDE protects data and log files, using AES and Triple Data Encryption Standard (3DES) encryption algorithms. Encryption of the database file is performed at the page level. The pages in an encrypted database are encrypted before they are written to disk and are decrypted when they're read into memory.

6. Physical & Environmental Security

For IFS internal physical and environmental security refer to the "IFS Information Security – Internal Controls" document which applies to IFS's own sites. Azure data center design and operational management is compliant with a broad range of international and industry standards including ISO 27001, FedRAMP, SOC 1, and SOC 2. Information on standards and certifications can be found at Azure Trust Center. They also are compliant with country or region-specific standards including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls which these standards mandate.

6.1. Physical Security Access Controls

Azure data centers used by IFS to provide IFS Customerville Services are designed, built and operated by Microsoft in a way that strictly controls physical access to the areas where IFS Customerville customer data is stored. Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the data center resources. 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. Based on the information made available by Microsoft, layers of physical security are:

- **Access request and approval**. Access must be requested prior to arriving at the data center. Visitors are required to provide a valid business justification for the visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by Microsoft employees. A need-to-access basis helps keep the number of individuals needed to complete a task in the data centers to the bare minimum. After Microsoft grants permission, an individual only has access to the discrete area of the data center required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire.

- **Facility's perimeter**. When arriving at a data center, visitors are required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the data centers, with a security team monitoring their videos at all times.

- **Building entrance**. The data center entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the data center and monitor the videos of cameras inside the data center at all times.

- **Inside the building**. After the visitor enters the building, they must pass two-factor authentication with biometrics to continue moving through the data center. If their identity is validated, they can enter only the portion of the data center that they have approved access to. They can stay there only for the duration of the time approved.

- **Datacenter floor**. Visitors are only allowed onto the floor that they are approved to enter. They are required to pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacenter without our knowledge, only approved devices can make their way into the data center floor. Additionally, video cameras monitor the front and back of every server rack. When a visitor exits the data center floor, they again must pass through full body metal detection screening. To leave the data center, they are required to pass through an additional security scan.

Microsoft requires visitors to surrender badges upon departure from any Microsoft facility. Information on physical security at Azure data center security can be found at Azure Trust Center.

6.2. Physical Security Reviews

Physical security reviews are conducted periodically of the data center facilities to ensure that they are running in accordance with the specified requirements. All personnel associated with hosting of the physical data center do not have electronic access to the Azure systems within the data center, nor do they have access to the Azure collocation room and associated cages.

6.3. Physical Disposal of Devices holding Data

Customer data is electronically wiped from virtual machines by destroying the encryption keys that protect it, thereby making it inaccessible. The physical storage device upon which data (virtual machine images, data storage files, etc.) are wiped in accordance with NIST 800-88 compliant deletion procedures. For any hardware devices that cannot be wiped (e.g. faulty equipment), these are physically destroyed so as to render recovery impossible. This process comprises one of disintegration, shredding, pulverizing, or incinerating. The method used is determined by asset type. Records are retained regarding the destruction.

7. Operations

7.1. Monitoring Platforms

Multiple monitoring platforms are used to support IFS Customerville Services operations.

Monitoring is used to manage and protect the infrastructure hosted in Azure. The monitor collects data from managed sources into central data stores. This data includes events and performance data. After the data is collected, it is used to support the generation of event alert and their subsequent analysis. The monitor also separates the collection of the data from the action taken on that data, so that all actions performed on the data are clearly identified and auditable.

IFS Customerville uses log analytics for central log and event management. Alerts are enabled using queries of logs to report unhealthy events and are sent to ITOps. Critical events are sent to staff on call.

In addition, 3rd party monitoring software is utilised to provide additional service and application monitoring and alerting capabilities to the operations. Websites provided by Customerville as part of the product are monitored for uptime and performance. Alerts are sent to staff on call to respond to incidents. Uptime and performance reporting is made available daily, weekly, and monthly.

7.2. Automation and Templates

Automation tooling is used to automate frequently repeated tasks so as to reduce likelihood of errors and speed up their execution. This includes routine housekeeping tasks that are scheduled at regular intervals as well as one-off activities such as initial service creation. Automation is used in conjunction with service templates so that consistency, and hence reliability of services is enhanced.

7.3. Backup and Recovery

IFS Customerville Services include a robust, multi-level backup and recovery solution which comprises geographically separated backup storage away from the production environment. Certain aspects of the solution resilience are provided by the Azure services themselves and are built into the IT architecture of Azure. These include redundancy of critical elements of the service including compute, storage, network, power and environmental elements with the ability to automatically recover from a low-level failure should a hardware component develop a fault. Such resilience is provided at both the primary production data center as well as the secondary, geographically separated data center where backup/recovery storage is held. IFS Customerville Services customers are able to choose the primary data center locations from a list of options, this then auto selects an appropriate secondary data center location based on IFS and Azure requirements. The physical separation of the two locations is in accordance with industry best practice so as to provide suitable protection against major events such as natural disasters etc.

Backups are monitored to ensure successful completion and recovery processes are tested regularly so as to ensure that an IFS Customerville Services can be restored following a major system failure.

Data retention varies based on the resource being backed up and requirements.

- Servers: 14 days
- Databases: 35 days + 5 weekly + 13 months

7.4. Disaster Recovery

Disaster recovery plans are in place for the IFS Customerville Services and are tested periodically to validate their effectiveness to recover a service in the event of a major failure. Backup and recovery services described in the previous section utilise the physical separation of the primary and secondary data center to enable the recovery of the service back to the primary data center or to a suitable alternative Microsoft Azure data center depending upon the nature of the disaster. In the event of a disaster where an entire Microsoft Azure data center becomes unavailable, re-configuration of the customer's connectivity into the service will be necessary and this will be assisted by IFS. Broader aspects of Disaster Recovery falling outside the scope of the IFS Customerville Service availability are a customer responsibility and need to be included within the customer's own Disaster Recovery planning and management processes.

7.5. Security Logging and Monitoring

IFS Customerville Services comprise security logging and monitoring at multiple levels. Microsoft Azure Log Analytics combined with Security Center provides logging with associated monitoring at the hardware and infrastructure layer, and alerts and associated remediations are provided by Microsoft as part of the Azure service delivery. The IFS Customerville IT Ops team monitor the health of the IFS Customerville Service at platform, application and network connectivity level, generating alerts using various monitoring tools that are reported to the IFS service management system for investigation and actioning as part of IFS Customerville Service management.

7.6. Malware Protection and Patching

The IFS Customerville Services includes the deployment of anti-virus and malware protection services to protect the service components held within the IFS Customerville Services. These protection services are updated regularly with the latest virus definitions to ensure that the service remains protected against constantly evolving threats.

Operating systems and infrastructure components that make up the service are regularly patched to keep them up to date with the latest security vulnerability patches. Such patching is performed in combination by Microsoft and IFS according to defined patching and maintenance responsibilities.

Patching of IFS products, either to correct errors or to address identified security vulnerabilities is performed by IFS in consultation with the IFS Customerville Services customer so as to ensure that there is no conflict with a customer's operational use of the IFS products.

Malware protection and patching of end user computing devices and customer IT infrastructure, including communications equipment within the IFS customers domain providing access to the IFS Customerville Services, is a customer responsibility and is not performed by IFS.

8. Communications

8.1. Customer connections to the IFS Customerville Service

IFS Customerville Services provide three different connection methods to the service, each suited to different situations:

- Flat file transmission over SFTP/FTPS (PGP encryption of files is supported)
- API

- Service bus

It is important that, whatever connectivity mechanism is chosen by the customer, it is reliable, secure and provides adequate bandwidth and acceptable latency. Not all IFS products support all connection methods, and selection of the appropriate method is agreed between IFS and the IFS Customerville Services customer either during the procurement or service implementation phase.

Flat File Transmission
IFS Customerville can accept flat files (.csv) from clients only over a secure connection method, either SFTP or FTPS. The client may also encrypt these files and a key exchange can be made with IFS Customerville to allow services to decrypt files. All data stored on secure FTP servers is encrypted at rest.

API
IFS Customerville provides an API for sending respondent data. The REST API provides a flexible system to manage survey invitations. You may query our system using simple URL syntax. REST API calls use the standard GET, POST, PUT or DELETE HTTP methods. IFS Customerville will provide an Authentication Token and define the data that will appear in the survey invitation. The Authentication Token is specified in the HTTP header X-API-TOKEN and provides the security authorization to send invitations to Customerville. All calls to the APIU are made over https (TLS). Unencrypted connections are prohibited.

Service Bus
IFS Customerville can provide clients with the ability to send respondent data over TLS to an Azure Service Bus. Azure Service Bus is a fully managed enterprise message broker with message queues and publish-subscribe topics (in a namespace). All connections made to the service bus and between the bus and applications are encrypted.

8.2. IFS Connection to Customer IFS Customerville Services

Connections from a client to IFS Customerville are done through three methods to support the sending of respondent data. Flat file transfers over SFTP/FTPS (PGP encryption of files is available), API over TLS, and Azure service bus over TLS. Storage for flat files is protected by encryption in transit and at rest, SFTP/FTPS is enforced, plain FTP is not allowed. API's are restricted to HTTPS and enforced through redirection. Azure service bus secure connections using TLS are enforced.

8.3. Internal Azure Communications

Communications between Azure internal components are protected with TLS encryption. In most cases, the X.509 certificates are self-signed. Certificates with connections that can be accessed from outside the Azure network are an exception, as are certificates for the Azure Fabric Controllers (FCs). FCs have certificates issued by a Microsoft Certificate of Authority (CA) that is backed by a trusted root CA. This allows FC public keys to be rolled over easily.

Azure implements host-based software firewalls inside the production network. Several core security and firewall features reside within the core Azure environment and which reflect a defence-in-depth strategy. Customer data in Azure is protected by the following firewalls:

Hypervisor firewall (packet filter): This firewall is implemented in the hypervisor and configured by the fabric controller (FC) agent. This firewall protects the customer's tenant that runs inside the Virtual Machine (VM) from unauthorized access. By default, when a VM is created to host the customer's IFS Customerville Services, all traffic is blocked and then the FC agent adds rules and exceptions in the filter to allow authorized traffic.

Native host firewall: Azure Service Fabric and Azure Storage run on a native operating system, which has no hypervisor and, therefore, Windows Firewall is configured with the appropriate sets of rules.

Host firewall: The host firewall protects the host partition, which runs the hypervisor that manages the Azure services utilised by IFS Customerville Services. The rules are programmed to allow only the FC and jump boxes to talk to the host partition on a specific port.

Firewalls that are implemented on all internal Azure nodes have three primary security architecture considerations:

- Firewalls are placed behind any load balancers and accept packets from anywhere. These packets are intended to be externally exposed and would correspond to the open ports in a traditional perimeter firewall.
- Firewalls accept packets only from a limited set of addresses. This consideration is part of the defensive in-depth strategy against DDoS attacks. Such connections are cryptographically authenticated.
- Firewalls can be accessed only from select internal nodes. They accept packets only from an enumerated list of source IP addresses.

9. IFS Customerville Service Development & Maintenance

9.1. IFS Product Development Testing

Security testing is performed at multiple stages within the development of an IFS Customerville Services. IFS Products themselves undergo extensive security testing during their development lifecycle within IFS Research & Development (R&D). Such testing checks for known security risks using industry best practice security frameworks including OWASP. The tests include checks for injection flaws, broken authentication, sensitive data exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), insecure deserialization, inclusion of components in the IFS Product with known vulnerabilities and lack of logging and monitoring facilities.

9.2. IFS Customerville Penetration Testing

In addition, IFS Customerville Services systems are tested on a dedicated, production grade environment hosted in Azure, built and maintained using the same architecture, design standards, tooling and processes employed in all IFS customers environments. The security testing environment comprises all standard, core product modules that are used to establish customer specific configured solutions.

Penetration testing of the IFS Customerville Services systems is performed annually or following any substantial change to the environment and is conducted by a trusted third-party security pen test partner. The penetration testing is conducted from the internet to replicate real world use cases. Both infrastructure and application testing is included within the testing scope. A formal report detailing issues found and associated severities is compiled as a result of the testing. Remediation and risk mitigation actions resulting from the penetration testing are identified and agreed corrective action plans established. Customer managed penetration tests are not permitted by IFS.

IFS Customerville Services customers may request a copy of the penetration tests performed on the same release or version that matches their deployment of the IFS Products as deployed in an IFS

Customerville Services solution. The report will be provided under an appropriate non-disclosure agreement only and will be for the customer's information only.

9.3. Vulnerability Management

IFS products and services are scanned for known security vulnerabilities. Threat intelligence sources are also utilised to identify known weaknesses in the service elements that make up IFS Customerville Services. As described above, known vulnerabilities in Azure infrastructure and platform services and IFS product infrastructure components are patched automatically as part of IFS Customerville Services management.

IFS Customerville services are scanned and monitored on a regular basis for vulnerabilities. Discovered vulnerabilities are tracked internally in a ticketing system and rated. Scans are conducted at least once per month and reviewed. Remediation efforts and work are recorded as comments in the ticket. Vulnerability scans will be run automatically using available tools and delivered to staff via email and automatically created as tickets. Vulnerabilities with a severity of critical are mitigated/resolved/remediated within 60 days of discovery.

10. IFS Secure Product Development Lifecycle

Customerville has two departments for code development. The Services department is responsible for client facing development, support, deployment, and maintenance of the product. The R&D department is responsible for product development, new features, and non-client specific support. The services department is comprised of Customerville Account Management Teams (CAT). Each CAT has clients assigned to them and they are responsible for those clients. R&D is comprised of the VP of Customerville R&D and a Program and Product Manager and the development team. A roadmap is developed by the VP, Product Manager, and architect according to the stakeholders requests. The Program Manager creates new stories for each sprint that R&D works on based on that roadmap. IT Operations (IT Ops) at Customerville provides support and maintenance for the Azure resources used to operate the product. All three departments work together to provide security around the development of the product.

Code is developed and tested in a separate environment that does not include production data. Access to all environments is controlled by IT Ops through tickets and approvals by managers. Staging of production code is done using a staging slot in production or a separate staging environment depending on need. Only two roles have access to deploy production code, trained team leads and CAT managers.

ITOps runs monthly vulnerability scans on the dashboard and survey product along with all virtual machines. Reports are saved as tickets with remediation, mitigation (if applicable) and acceptance status of known vulnerabilities. Weekly vulnerability scans are conducted on Azure SQL databases and reported as tickets.

11. Information Security & Third Parties

IFS operate formal supplier management policies and process which help govern the security of the products and services they provide. From supplier selection, through onboarding and including the day-to-day management of the supplier relationship supplier security is a key aspect of the supplier management process. Such processes include the use of supplier security questionnaires as well as the validation and inspection of any security certifications that may be held and are applicable to their scope of supply.

IFS Customerville Services is dependent upon very few suppliers for service delivery, the main supplier being Microsoft with the provision of the Azure service upon which IFS Customerville Services solutions run. IFS and Microsoft operate in close partnership and supplier management includes frequent meetings between the two parties at both a strategic and operational level. Defined routes for issue escalation exist as well as priority support should a significant incident occur.

12. Incident Management

In accordance with its contractual, legal and regulatory obligations, IFS notify impacted customers without undue delay of any unauthorized disclosure of their respective customer data by IFS of which IFS becomes aware to the extent permitted by law.

IFS Incident Management processes have been designed to ensure that forensic information is preserved during the investigation of a security incident. IFS will not share information regarding the details nor nature of the incident other than with impacted parties unless it is required to do so.

13. Compliance

13.1. Audits and Reviews

Numerous audits and reviews are conducted on multiple service elements that make up the IFS Customerville Services. Such audits and reviews are conducted by both IFS internal independent audit and review teams as well and external consultancies and accredited organisations. The IFS Information Security Management System, including the IFS Cloud Security Management system is reviewed annually by external specialist agencies. This features as part of IFS' commitment to continuous improvement in the area of information security of its products and services and the assessments are conducted in accordance with industry best practice security frameworks including AICPA SSAE18 and ISAE 3000 SOC 2 Reporting.

As part of IFS supplier management processes, IFS reviews the security credentials of its suppliers, ensuring that they meet IFS requirements as part of the supplier onboarding process as well as ensuring that are maintained, which frequently includes validation of compliance by an accredited organisation in accordance with the suppliers' certifications.

13.2. Microsoft Azure Compliance and Certifications

Various audits and certifications apply to the Microsoft Azure Platform details of which can be found here: Azure Trusted Cloud Compliance. The following key security and privacy-related audits and certifications are:

- ISO27001 – Information Security Management
- ISO27018 – Information Technology Security
- SOC 1, 2, and 3 – System and Organization Controls Reports
- Cloud Security Alliance (CSA) STAR Certification

Further information can be found on Microsoft's Trust Center.

13.3. Exclusions

IFS Products, including IFS Customerville Services, by their nature can be used for many different business purposes. Some of these relate to regulated industries requiring particular certifications. IFS do not certify its products or services in accordance with such regulations and certifications, this being a customer responsibility as part of their procurement process and due diligence regarding supplier and product selection.

14. Data Processing

This section identifies the data processing performed in connection with the operation and maintenance of the IFS Customerville services including the sub-processors involved. Sub-processors involved with the implementation of the solution are not included within this document since they may vary on a customer-by-customer basis and consequently will be described in a separate statement of work.

14.1. IFS Affiliates

IFS Affiliates located in the EEA

Entity name	Reg no	Service description	Data Processing (see Section 4)	Control Measures	Country
IFS World Operations AB	556040-6042	Corporate Functions	Global IT Support	Intragroup Agreement including SCCs IFS ISMS	Sweden

IFS Affiliates located outside the EEA:

Entity name	Reg no	Service description	Data Processing (see Section 4)	Control Measures (see Section 5)	Country
IFS World Operations AB UK Branch	FC039108	IFS Corporate IT, Cloud Services	Global IT Support IFS Cloud Services R&D Product Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	United Kingdom
IFS North America, Inc.	39-1292200	IFS Corporate IT	Global IT Support	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	USA
IFS R and D International (Private) Ltd	PV 15891	R&D, Global Support, Cloud Services	Product Implementation Product Support, IFS Cloud Services	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Sri Lanka
Industrial & Financial Systems R&D Ltd	PB 1274	R&D, Global Support, Cloud Services	Product Implementation Product Support, IFS Cloud Services	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Sri Lanka
IFS Research and Development (Private) Ltd	PV 14786	R&D, Global Support, Cloud Services	Product Implementation Product Support, IFS Cloud Services	Intragroup Agreement including SCCs IFS ISMS Site to Site VPN encryption of the IFS private network	Sri Lanka

14.2. Global Third-party Sub-processors

Global Third-party service providers located in the EEA

None

Global Third-party service providers located outside the EEA

Entity name	Service description	Data Processing (see Section 4)	Control Measures (see Section 5)	Country
Microsoft Corporation	Cloud platform services	Azure Service Provision	Microsoft DPA	Data center location will be specified

			MS Key Vault secure management of Encryption keys within the EU	in the contract with customer
TATA Consultancy Services Limited	Consulting services	IFS Cloud Service Support	IFS Partner DPA Management in accordance with IFS ISMS IFS Monitoring & Detection Containerised environments managed by IFS	India
ServiceNow	Support platform	IT Service Management Toolset	Service Now DPA Security Management System certified in accordance with ISO 27001, SOC 2 Type 2 report	Netherlands & Ireland

14.3. Third-Party Software and Software as a Service Providers

Entity name	Service description	Country
Twilio - Sendgrid	SMTP/SMS Provider	USA
Lexalytics	Sentiment analysis	USA
Pro-IP	Geolocation services based off IP	Romania

14.4. Data Processing Descriptions

Project Implementation

In order to support the customer with the implementation of an IFS solution, IFS performs a range of activities, each of which may result in the processing of customer data. Such activities are performed by the IFS regional consulting team for the country in which the solution is to be implemented and may involve the support of other regional consulting teams and IFS Research and Development (R&D) staff as shown in section 1 above. IFS regional and global support teams may also be involved in the implementation phase in resolving any product defects identified during the implementation. IFS follow a standard implementation process using standardized implementation toolsets comprising the following activities:

- Discussion of business processes and practices;
- Design of system customisations;
- Design of Information System interfaces between existing/legacy IT systems used by the data exporter and the new solution;
- Processing of customer production data, including end user information to support data take-on/data migration activities to prepare the product for operational use;
- Processing of customer production data to support end user training;
- Processing of customer production data to support setup for solution verification and validation activities by the customer;
- Processing of customer production data to support the establishment of one or more reference environments to support system testing and live system maintenance and support;
- Processing of customer production system transaction data to support the investigation of a perceived system error or software bug pre-production.

Product Support

In order to implement the customer's IFS support agreement, IFS regional support teams and the IFS Global Support Organisation may require access to customer production or reference environments containing customer production data in order to investigate reported software issues associated with the IFS product. The investigation of certain product issues may require the involvement of IFS R&D.

IFS Cloud Services

Where IFS customers choose the IFS Cloud service, their IFS products that form their solution are hosted in Microsoft Azure datacentres. For European customers, these data centres will be located within the EEA in order to limit the extent of any transfers of personal data outside of the EEA. Selection of the datacentres that form the solution is made with the agreement of the IFS customer.

The Managed Services Team access the customer environment in Azure in order to perform the services included in the customer's managed services agreement only. Each service comprises the following primary activities:

- Creation of the Azure platform upon which the customer's solution will run;
- Installation of the IFS products that make up the customer solution;
- Configuration of the solution including the establishment of system performance monitoring;
- Monitoring of the system to ensure that it is compliance with its agreed service levels;
- Execution of backups to a secondary data centre, including performing recovery operations should a significant system failure occur;
- Proactive and reactive maintenance activities to address system monitoring alerts and system issues reported by the customer's end users. Such activities include software patching at operating system, middleware and application levels, database administration (where applicable) and performance tuning;
- System changes and enhancements, either to ensure the solution operates in accordance with its service levels or as a result of an agreed change with the customer;
- Service de-commissioning in accordance with a process agreed with the customer.
- Management of encryption keys where a customer has elected to have IFS perform this function for them.

The IFS Cloud Services team are not required to process customer data as part of their day to day activities. They do however hold administrative level permissions for the hosting environment in order to execute their technical responsibilities of maintaining the Azure platform the associated IFS products.

Azure Service Provision

The Azure data centers are managed and maintained by Microsoft in accordance with their ISO 27001:2013 and SOC 2/SOC 3 certified processes. Their responsibilities are to ensure the Azure services utilized by the IFS Managed Cloud solutions remain available and performing in accordance with their specification. The Azure services consumed by the IFS Managed Cloud solutions include:

- Infrastructure as a Service (IaaS) processing, storage, site recovery and network services;
- Platform as a Service (PaaS) database and web services for IFS products which do not require special platform management

Microsoft do not have access to applications within the virtualized environments within which the IFS products that make up our customer solutions run. They therefore do not have access to customer production data held within IFS Cloud solutions. However, since Microsoft staff have elevated permission access to the components of the Azure environment it is theoretically possible that they could process customer data (e.g. by monitoring traffic across a LAN segment of a particular data center in order to investigate performance issues). Microsoft's processes for managing the Azure data centers employ segregation of duty principles that make it extremely difficult to associate information on the physical Azure infrastructure with a specific Azure customer. Consequently, customers have the opportunity if they wish to manage encryption keys themselves rather tbhan have Microsoft perform this for them.

Global IT Support

The IFS Corporate Services business unit is responsible for providing IFS' global IT services which include all IFS mission and business critical IT systems, infrastructure and end user IT equipment that support our global business operations. IT Service Management is mainly provided out of the United Kingdom and Sweden, with IT operations, application and end user support provided from Sri Lanka. Corporate Services do not process customer data, instead they implement and maintain the internal IT services and equipment that support the IFS business operations. Whilst this includes the use of administrative level accounts, it does not include access to customer solution application accounts.

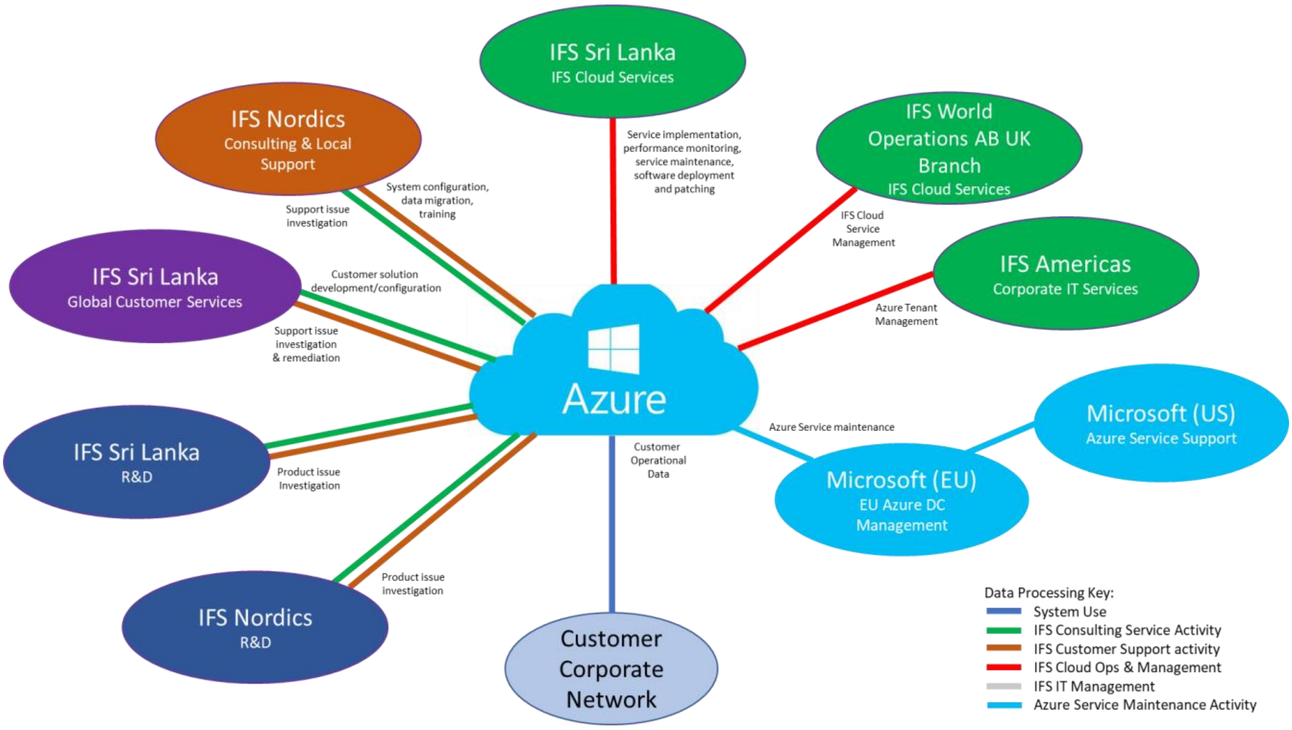
IT Service Management Toolset

ServiceNow is the Gartner Magic Quadrant leader IT Service Management Tool used by IFS to manage customer support tickets relating to its products and services. The system holds the user identity and business mail address of the nominated few customer users authorised to raise support tickets (typically 5). No customer production data is held within the ticketing system, only details of perceived issues associated with the IFS Cloud service. Ticket Data is held within the EU (Ireland and the Netherlands). Further information can be found in the ServiceNow Cloud Security FAQ document attached below.

PDF ServiceNow FAQ   PDF ServiceNow FAQ

14.5. Data Flows

The following diagram shows the data flows between each entity associated with the implementation and support of the IFS Customerville solution:


IFS Sri Lanka
IFS Cloud Services
IFS Nordics
Consulting & Local Support
IFS World Operations AB UK Branch
IFS Cloud Services
Service implementation, performance monitoring, service maintenance, software deployment and patching
System configuration, data migration, training
Support issue investigation
IFS Cloud Service Management
IFS Americas
Corporate IT Services
IFS Sri Lanka
Global Customer Services
Customer solution development/configuration
Azure Tenant Management
Support issue investigation & remediation
Azure
Microsoft (US)
Azure Service Support
Azure Service maintenance
IFS Sri Lanka
R&D
Customer Operational Data
Microsoft (EU)
EU Azure DC Management
Product issue Investigation
Product issue investigation
IFS Nordics
R&D
Customer Corporate Network
Data Processing Key:
System Use
IFS Consulting Service Activity
IFS Customer Support activity
IFS Cloud Ops & Management
IFS IT Management
Azure Service Maintenance Activity

Document Revision History

Rev.	Date	Owner	Remarks
1	13/05/2022	Todd Williams	Initial version

Distribution & Document Handling

This document is intended for use by IFS customers and partners and the contents is confidential to IFS.

Authorisation & Approval

This version of the document has been approved by the Owner and authorized for release by the Approver shown on the front cover of this document.

Review & Amendment

This document is reviewed on an annual basis and updated with evolving internal and external requirements and supplier arrangements. This document is subject to change without prior notice and such changes will be performed in accordance with IFS change management processes.

ABOUT IFS

IFS develops and delivers enterprise software for customers around the world who manufacture and distribute goods, maintain assets, and manage service-focused operations. We offer applications that enable companies to respond quickly to market changes and use resources in a more agile way to achieve better business performance and competitive advantages. IFS's products are known for being user friendly, modular in their design and flexible enough to support the customers in their way of working according to their established processes.

Learn more about how our enterprise software solutions can help your business today at ifs.com

Be your best in your Moment of Service!

WHERE WE ARE

AMERICAS
+1 888 437 4968

ASIA PACIFIC
+65 63 33 33 00

EUROPE EAST
+48 22 577 45 00

EUROPE CENTRAL
+49 9131 77 340

UK & IRELAND
+44 1784 278222

FRANCE, BENELUX AND IBERICA
+33 3 89 50 72 72

MIDDLE EAST AND AFRICA
+971 4390 0888

NORDICS
+46 13 460 4000

COPYRIGHT @2020 INDUSTRIAL AND FINANCIAL SYSTEMS, IFS AB, IFS AND ALL IFS PRODUCTS AND SERVICES NAMES ARE TRADEMARKS OF IFS. ALL RIGHTS RESERVED. THE NAMES OF ACTUAL COMPANIES AND PRODUCTS MENTIONED HEREIN MAY BE THE TRADEMARKS OF THEIR RESPECTIVE OWNERS.