Unified Support - Security Operations Center

(UniSup - SOC)

Table of Contents

IFS Cloud Security

Overview

As IFS continues to embrace Cloud Services, ensuring security in the cloud is essential for protecting data, applications, and infrastructure. By applying stringent security measures, IFS protects customer environments from threats, ensures compliance, and mitigates risks related to cyberattacks.

Intended Audience

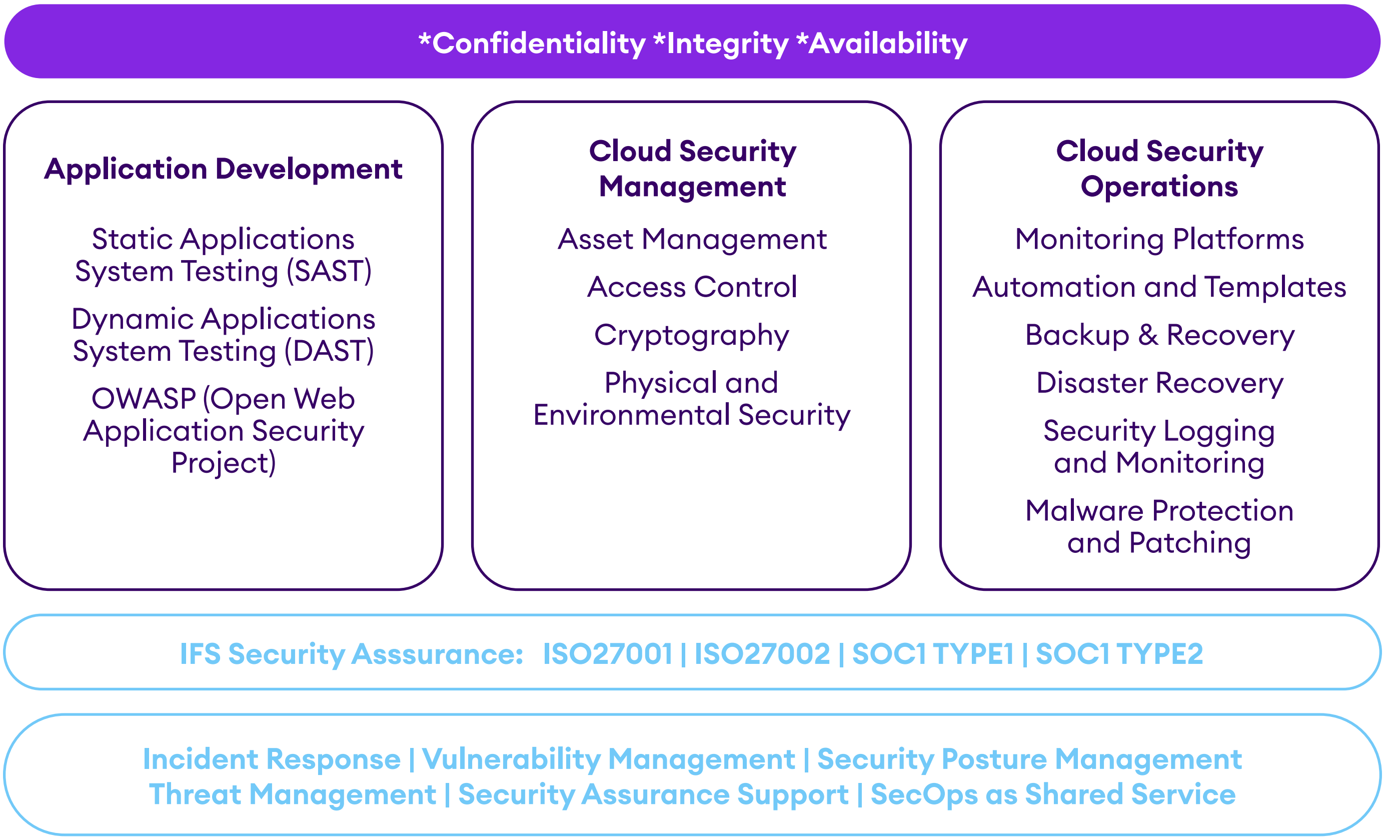
This document is mainly intended for IFS customers who are involved in implementing, supporting, and administering IFS solutions. The reference material provided here details key cloud concepts, roles, responsibilities, process descriptions, and various support tools to aid customers throughout their journey with IFS.

How is Cloud Security important to IFS?

IFS emphasizes safety, transparency, and industry-leading practices in information security, making it well-suited to the needs of cloud customers. Ensuring cloud security is essential for customers who have subscription-based software access, as it guarantees the confidentiality, integrity, and availability of their data. By preventing breaches, sustaining trust, adhering to regulations, and ensuring business continuity, cloud security serves as a catalyst for IFS in safeguarding customer data.

Security Strategy

At IFS, we employ a comprehensive "defense-in-depth" approach, featuring several layers of interlocking security protocols. Our aim is to safeguard customer data at every stage, while maintaining optimal availability. Here's how we accomplish this:



*Confidentiality *Integrity *Availability

Application Development

Static Applications System Testing (SAST)

Dynamic Applications System Testing (DAST)

OWASP (Open Web Application Security Project)

Cloud Security Management

Asset Management

Access Control

Cryptography

Physical and Environmental Security

Cloud Security Operations

Monitoring Platforms

Automation and Templates

Backup & Recovery

Disaster Recovery

Security Logging and Monitoring

Malware Protection and Patching

IFS Security Asssurance: ISO27001 | ISO27002 | SOC1 TYPE1 | SOC1 TYPE2

Incident Response | Vulnerability Management | Security Posture Management
Threat Management | Security Assurance Support | SecOps as Shared Service

Perimeter Security

This is the outermost layer of IFS customer security defense. Components include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and other boundary protection measures. Its primary goal is to monitor and filter traffic entering and leaving the network perimeter.

Network Security

IFS is Focused on securing the internal network infrastructure. Utilizes technologies like network segmentation, VLANs (Virtual LANs), and VPNs (Virtual Private Networks). Aims to control access and limit lateral movement of attackers within the network.

Endpoint Security

IFS Protects individual endpoint devices (e.g., laptops, desktops, servers, mobile devices). Solutions include antivirus software, endpoint detection and response (EDR), and mobile device management (MDM). Defends against malware, ransomware, and other threats targeting endpoints.

Identity and Access Management (IAM)

IFS Manages access to resources based on user identities and roles. Implements measures such as strong authentication, access control lists (ACLs), and privilege management. Prevents unauthorized access to sensitive data and systems.

Application Security

At IFS, we ensure application security with a structured process: Development teams adhere to security guidelines, integrate security requirements into design, and perform source code scans for OWASP top ten, SAST, and DAST vulnerabilities. Developers also use security plugins while coding.

Access Control

At IFS, we take security seriously. To safeguard your data and maintain a robust system, we adhere to the following access control strategies: apply Access Controls Checks Consistently, Multi-factor authentication for user authentication, apply the Principle of Least Privilege, avoid Direct Object References for Access Control Checks, avoid Unvalidated Forwards or Redirects.

Data Protection

Customer data is our top priority. We employ encryption techniques to safeguard data both in transit and at rest. This ensures that sensitive information remains confidential and integral throughout its lifecycle.

Encryption

At IFS, we offer customers data encryption– sophisticated protection for customer data. We collaborate with our cloud service provider to deliver secure encryption to our customers.

Monitoring

Our security operations center (SOC) constantly monitors network traffic, system logs, and user activity. Any suspicious behavior triggers alerts, allowing us to respond swiftly and mitigate potential risks.

Availability

High availability is essential for business continuity. At IFS we maintain redundant systems, failover mechanisms, and disaster recovery plans. Both RTO and RPO objectives are included in the customer's contract for each customer DR plan. In case of any disruptions, our services remain accessible to customers.

Regular Audits and Assessments

IFS conducts periodic security audits, vulnerability assessments, and penetration testing. These proactive measures help identify weaknesses and allow us to address them promptly.

User Awareness/Acceptable Usage

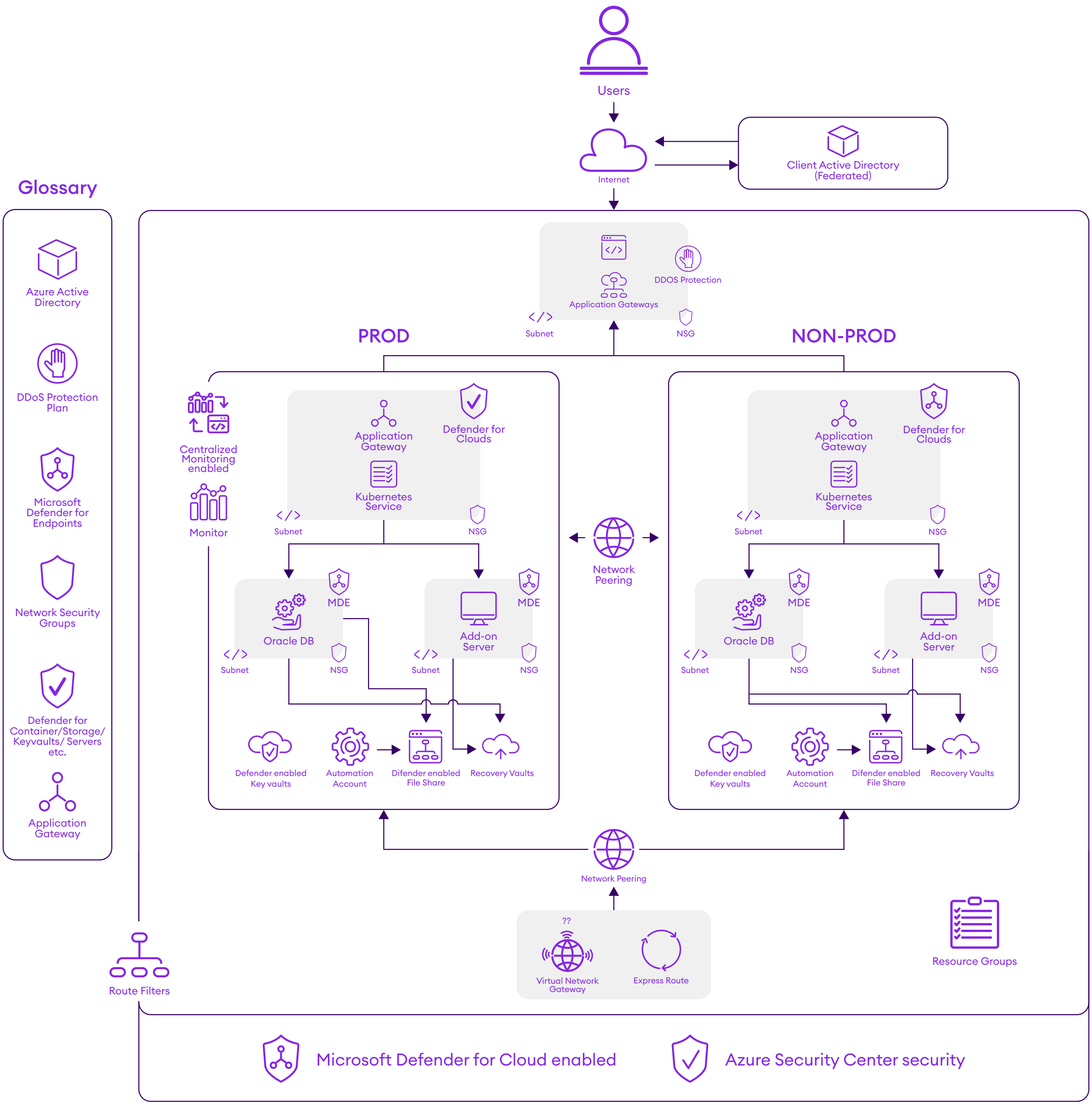
IFS has its own Academy to train its employees, customers, and partners. Other than that, IFS provides reputable third-party training for our employees.

By combining these strategies, IFS ensures that customer data remains secure, reliable, and available.

At IFS, our Cloud Environments are intentionally separated from the IFS corporate network and customer networks. It basically provides segregated and private user accounts for each customer.

While customers use the same version of the software, their data remains separate and secure. IFS collaborates with Microsoft to enhance its services.

The security overview provided in the diagram below outlines the high-level view of the security measures implemented by IFS.



IFS prioritizes security by leveraging established technologies with well-known security properties.

Additionally, IFS employs security orchestration to automate incident response processes within the organization

IFS Cloud Security Services

At IFS we have our own security operations center team, who is committed to complying with IFS Information Security policy and procedures to enhance Cloud Security Posture. The IFS Unified Support - Security Operations Center (US-SOC) team is focused on providing Information Security services towards IFS Cloud customer Products & Infrastructure. The primary focus of the UniSup-SOC team would be to monitor and manage information security events of IFS customers.

Incident Response

Responsible for proactively monitoring and managing Information Security Events & Incidents of IFS customers Cloud Service Deployments. In IFS, our Cloud Security Incident Response Service focuses on risk assessment, structured procedures, and transparency, ensuring a reliable and secure environment for our customers.

Monitoring cloud environments for anomalies

- Use monitoring tools to track various metrics across your cloud resources.
- Set up alerts for thresholds to proactively identify issues.

Detect anomalies

- Leverage anomaly detection techniques:
  Statistical Methods: Detect deviations from expected patterns using statistical models
  Machine Learning Models: Train models to recognize abnormal behavior based on historical data.
  Behavioral Analysis: Understand normal behavior and flag deviations.

Analyze and Response

- When an anomaly is detected:
  - Investigate: Understand the root cause.
  - Severity Assessment: Determine the impact (critical, major, minor).
  - Response Plan: Define actions based on severity.
  - Automated Responses: Implement automated actions (e.g., scaling resources, restarting services).
  - Manual Responses: Escalate to relevant teams for further investigation.

Incident Management

IFS follows a well-structured incident management process to handle security incidents effectively:

- Incident Identification:
    - IFS actively monitors its systems for any signs of incidents.
    - Incidents can include security breaches, service disruptions, or anomalies.
- Incident Triage:
    - When an incident occurs, IFS prioritizes it based on severity.
    - Critical incidents receive immediate attention, while minor ones may be addressed later.
- Resolution:
    - IFS works swiftly to resolve incidents.
    - This involves investigating the root cause, implementing corrective actions, and restoring normal operations.
- Post-Incident Review:
    - After resolving an incident, IFS conducts a thorough review.
    - The goal is to understand what happened, identify areas for improvement, and enhance processes.

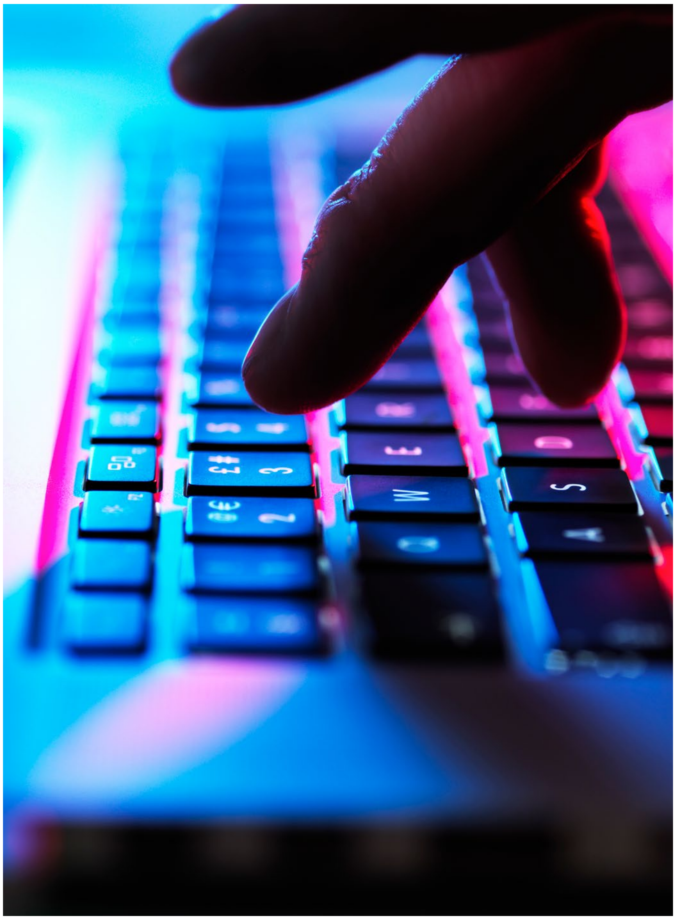
Vulnerability Management

We take necessary steps to identify and remediate Information Security vulnerabilities in IFS customer infrastructure. Our vulnerability management program contributes to a secure and resilient environment for our customers.

- *Regular Scanning*: Continuously scan for vulnerabilities in the customer infrastructure.
- *Prioritization*: Assess identified vulnerabilities based on severity and impact.
- *Immediate Remediation*: Take prompt actions to address critical vulnerabilities.
- *Adherence to Security Policies*: Align with IFS's security policies.

OS patches Management

Critical OS patches require research and testing prior to deployment. IFS reviews these critical OS patches as soon as it is generally available for public, and they promptly applied for the applicable hosted operating systems.



At IFS, the security and reliability of your services are our top priorities. Hence our planned Platform Maintenance windows will apply the IFS Cloud Service Planned Maintenance Policy to apply the OS patches. Our planned maintenance schedules are thoughtfully chosen to mitigate disruption and are communicated via the IFS Service Center banner.

Penetration Testing (Pentest)

Our cybersecurity and technology never stand still. We perform extensive penetration testing annually of our IT systems and networks with a reputed third-party external specialist. Customers can request the outcome of a test by raising a request via our customer portal, as explained in the active customer engagement section.

Security Posture Management

Making sure the Information Security postures are continuously evaluated and improved with the collaboration with IFS customers.

- Customers play a crucial role in incident reporting. When they encounter security incidents or anomalies, timely reporting allows IFS to investigate and respond promptly.
- IFS collaborates with customers to share security assessments, penetration testing findings, and vulnerability scans findings with customers.
- IFS actively seeks feedback from its customers regarding security practices, concerns, and suggestions.

Scheduled maintenance

As part of our commitment to providing you with the best experience, we periodically schedule maintenance windows. These windows allow us to update and enhance your Subscription Services, ensuring you can take advantage of new features and functionality. All the relevant information will be published through CSM portal.

Threat Management

IFS's proactive threat management minimizes risks and ensures a secure environment for our customers.

- Threat Detection:
  - » At IFS we actively monitor your systems for potential threats. Detection mechanisms include security tools, logs, and anomaly detection. Our goal is to identify any abnormal behavior or security incidents.
- Analysis of Detections:
  - » When threats are detected, we analyze them promptly. This involves understanding the nature of the threat, its impact, and potential vectors. Threat analysts assess the severity and prioritize actions.
- Immediate Mitigations:
  - » We take swift action to mitigate threats.
- Our responses may include:
  - » Blocking malicious IPs.
  - » Applying security patches.
  - » Isolating affected systems.
  - » Notifying relevant teams.

Compliance and Certification

IFS's commitment to annual compliance assessments ensures that information security practices remain up-to-date and aligned with industry standards. IFS demonstrates its dedication to maintaining a secure and compliant environment.

- ISO27001
- SOC 1 Type I / SOC 1 Type II Reports, Bridge Letter
- Annul Pentesting

Customers can conveniently request these assessments through the Customer Success Management (CSM) portal (IFS Service Center portal), streamlining the process and enhancing transparency.

IFS DevSecOps Practice

IFS DevSecOps bridges the gap between development, security, and operations by embedding security practices into the **DevOps** workflow. By doing so, it reduces the risk of deploying software with misconfigurations and other vulnerabilities that bad actors can exploit. IFS also enhances customer security by adopting DevSecOps practices.

Release Management and Service Update

At IFS we periodically release updates for the Subscription Software. Our focus is on improving known bugs, enhancing features, and developing the data security of our products. Therefore, we recommend that all IFS customers update their environment as soon as we release these updates. All customers receive release notifications through the CSM portal or, via the IFS Community Page when these updates become available.

Active customer engagement

IFS customers can engage when facing security-related issues or requesting information:

Reporting an Information Security Incident

- When a customer identifies an information security incident (e.g., malware, DDoS attack, unauthorized access) you can reach us directly.
  - » *Action*: Open an incident or request through the CSM Portal (IFS Service Center portal).
  - » *Details*: Provide relevant information about the incident.
  - » *Unified Support Security Operation Center*: They will assist promptly.

Request the support for the vendor assessment

- Request for Information or Security Queries
  - » When a customer needs specific information (e.g., security compliance documents, penetration test reports): *Action*: Use the CSM Portal to request the necessary documents. *Prompt Response*: Our Unified Support Security Operation Center will provide the requested information.
- At IFS we proactively engage with customers to provide support for vendor assessments when you newly purchase our products.

Policies and processes

IFS has established comprehensive security policies aimed at safeguarding the confidentiality, integrity, and availability of Subscription Services. We diligently train all relevant IFS personnel, emphasizing their responsibility to adhere to these policies. Additionally, procedures are meticulously documented in alignment with these principles. IFS Trust Center

Definitions

Availability or "system availability" refers to a condition where the Cloud Environment is accessible. IFS's goal is to provide system availability 24 hours per day, 7 days per week, except during periods of scheduled maintenance.

Application Support means support for application-level incidents where the Cloud Environment is available, but there is a business interruption or a request for assistance in the production system.

Bridge Letter, also known as a "gap letter," is made available by IFS to cover a period of time between the reporting period end date of the most current System and Organization Controls (SOC) report and the release of a new SOC report. This typically occurs because a SOC report covers only a portion of a fiscal year.

Change means the addition, modification, or removal of anything that impacts the configuration of the Subscription Software within the customer-facing Cloud Environment.

Cloud Environment refers to the application hosting environment and infrastructure platform on which the Subscription Software and Service Availability Data are hosted and to which the Subscription Services apply.

CSM Portal refers to the IFS Support portal that provides customers with the ability to log issues, search the Product Knowledge Base, participate in IFS Support Communities, view IFS contacts, pay invoices, and other self-service functions available to all IFS Support customers who have a valid Support/ Subscription Services agreement in place with IFS.

Customer, **customer**, **you**, or **your** refer to the IFS customer who has purchased a subscription to access and use the Subscription Software and Subscription Services from IFS or an IFS-authorized partner or distributor.

Customer Data means the Information provided, entered, or uploaded for use by or with the Subscription Software by the customer or its authorized users.

IFS, **our**, or **we** refers to IFS (US), LLC or one of its affiliates (including their respective predecessor companies) that has entered into an applicable subscription agreement with the customer.

IFS Community means an online channel available through internet which enables customers to communicate with their peers who have subscribed to the same Subscription Software.

Instance refers to a virtual server configuration accessible from a designated URL, and on which the Subscription Software and Customer Data are hosted for a group of IFS customers utilizing a multi-tenant cloud application.

Knowledge Base or **IFS Knowledge Base** means the centralized repository of Information specific to Support for the Subscription Software.

Managed Services means software or consulting services that IFS provides to the customer to manage the applicable Subscription Software as contemplated under a Managed Services agreement or other ordering document. Managed Services are not a component of the Subscription Services.

Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time and is the point in time to which data will be recovered.

Recovery Time Objective (RTO) describes the duration of time within which Subscription Services will be restored following a declared disaster.

Subscription Services means the Subscription Software-related application hosting services and Support that IFS provides to a customer under an applicable agreement.

Subscription Software means, collectively or individually, the computer software programs identified in the applicable order form or other ordering document for which IFS is providing the Subscription Services (and may be referred to in a legacy subscription agreement as products, software products, software, programs, or licensed programs).

Support means IFS's then-current standard maintenance and support services for its eligible Subscription Software and may be referred to herein as "support," "maintenance," or "maintenance and support." "Support" may also be used generically to refer to the IFS Support organization, as applicable.

Useful links

About us: IFS Home Page

Major incident status information is reflected on the: IFS CSM Portal (Support Portal)

You can start discussion with our community via IFS Community Page

Explore how we comply legally: IFS Legal Page

Details about Infor's Cloud Security can be found at IFS Trust Center

Our support operation handbooks: IFS Documentation

Registration for the Introduction to Customer Success and Next Steps in the Cloud webinar can be found here.

About IFS

IFS develops and delivers enterprise software for companies around the world who manufacture and distribute goods, build and maintain assets, and manage service-focused operations. Within our single platform, our industry specific products are innately connected to a single data model and use embedded digital innovation so that our customers can be their best when it really matters to their customers–at the Moment of Service™.

The industry expertise of our people and of our growing ecosystem, together with a commitment to deliver value at every single step, has made IFS a recognized leader and the most recommended supplier in our sector. Our team of 4,500 employees every day live our values of agility, trustworthiness and collaboration in how we support our 10,000+ customers.

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

#MomentOfService

Production: IFS, November 2024.