PUBLIC

IFS Copperleaf Service Controls

Copperleaf ISMS

Date:	21/03/2025
Revision:	1
Owner:	VP, InfoSec & Technology
Approved By:	SVP, IT Cyber Security

Contents

1. Copperleaf Security Management

IFS Copperleaf's commitment to protecting its information security as well as that of its staff, customers, partners, and suppliers stems from senior leadership of Copperleaf, supported by IFS executives and the Board. As a member of the IFS Group, Copperleaf benefits from the harmonised IFS Global ISMS while tailoring controls to Copperleaf customer use cases and requirements. Adopting a risk-based approach in accordance with best practice, Copperleaf have adopted the ISO 27001 and SOC 2 frameworks upon which to base the Copperleaf Information Security Management System ("ISMS"). As the most internationally recognized security standard, ISO 27001 sets a high bar thus helping ensure that the security controls and practices used by Copperleaf best serve to protect the interests of all Copperleaf stakeholders including customers and partners. Compliance with SOC 2 allows Copperleaf customer assurance of the security of cloud services provided by Copperleaf ("Copperleaf Services").

Copperleaf have developed and continually improve this ISMS covering all aspects of the Copperleaf Services. The Copperleaf ISMS covers the following key areas of the service:

- **Application & Data Access Management** – Processes to ensure approvals and reviews of role-based access are required for those staff with access to customer services and confidential information. Only those with a defined role in the providing of Copperleaf Services to a customer are permitted access.

- **Cloud Platform Management** – Processes to manage the provisioning, maintenance, security, and deprovisioning of cloud services underpinning the Copperleaf Services.

- **Physical & Environmental Protection** – Processes to manage physical access to infrastructure (servers, workstations, and other network devices) and to manage the environmental protections (power, cooling, and fire prevention) of the infrastructure.

- **Personnel Security** – Processes to ensure the qualification, appropriateness, and performance of staff assigned to roles providing Copperleaf Services.

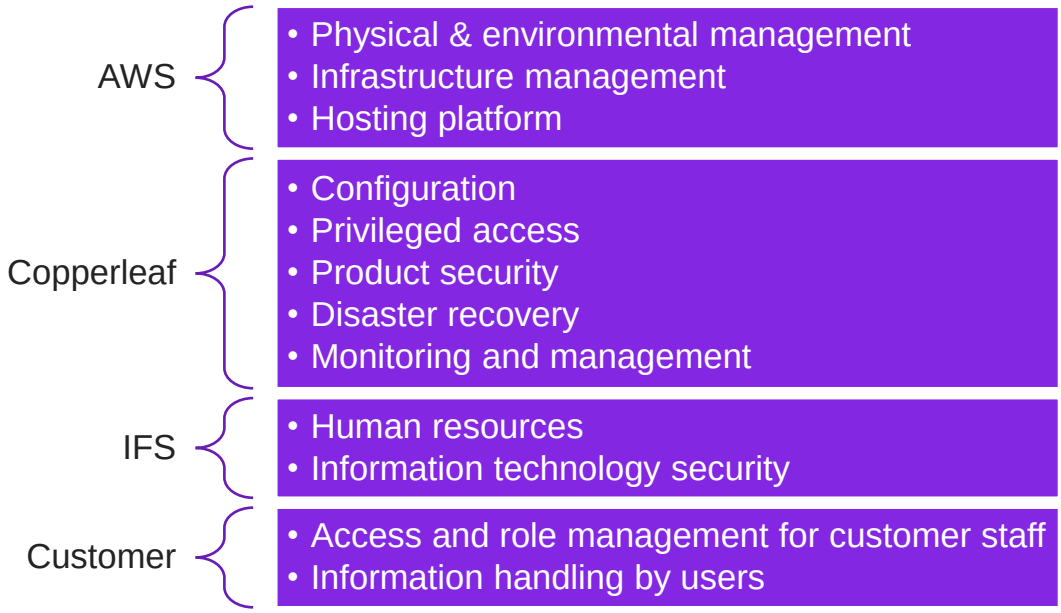
2. IFS Copperleaf Security Architecture

Copperleaf Services are deployed upon Amazon Web Services ("AWS") and are available in a subset of AWS's global data centres, allowing customers to select a suitable location for their specific requirements, considering factors such as network latency, data sovereignty, etc. The service comprises a primary and secondary data centre, the latter being used to facilitate the associated backup and recovery services described in more detail in section 7.4 below.

The security architecture of Copperleaf Services is constructed of four segments:

- Amazon Web Services security management
- Copperleaf Services specific security management
- IFS security management
- Customer security responsibilities

Each component is required to securely manage information and assets within the hosted Copperleaf Services. High-level responsibilities are shown in the following diagram, and details are given in this document and the Copperleaf SOC 2 Type 2 report.



3. Asset management

3.1. IT Assets

Physical IT assets used in delivering Copperleaf Services are currently provided by Amazon Web Services ("AWS"). These assets are in AWS data centres that are designed for resiliency and security. All aspects of the physical security of IT assets providing Copperleaf Services are managed by AWS. Staff employed by AWS to maintain data centres and physical assets are subject to background checks and monitoring for compliance with security policies. Copperleaf utilizes AWS services based on the "Nitro" hypervisor, which provides a security feature preventing AWS staff with physical access to servers or other infrastructure from being able to perform any action which would give them access to AWS customer data.

AWS operates a shared security model where AWS and Copperleaf maintain and perform specific security controls that work together to maintain the security of Copperleaf Services. Virtual IT assets supporting the AWS environment are managed by AWS staff. These staff are also subject to background checks and monitoring for compliance to security policies.

IT assets in the form of AWS services consumed by Copperleaf, that form the basis for the hosting of Copperleaf Services, are managed by the Copperleaf team using AWS-provided tools and interfaces. An inventory of all such assets is held in a Configuration Management Database (CMDB) by Copperleaf. Such assets are only managed by the relevant Copperleaf personnel who are responsible for asset provisioning, operational monitoring, maintenance, and deprovisioning once no longer required.

Customer onboarding comprises the provisioning of the AWS virtualised services that host the specific Copperleaf 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. IP allowlist, virtual private network, etc).

During the life of the Copperleaf solution, the Copperleaf team are responsible for the monitoring and maintenance of the cloud 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 Copperleaf's service management tools.

At the end of life of a Copperleaf Service, all deployed cloud assets comprising the service are securely destroyed using the NIST-recommended administrative processes provided by AWS, and which are certified in accordance with ISO 27001 and SOC 2, as well as other internationally recognised security standards (please see AWS's Compliance Programs site for more details).

3.2. Information Assets

Copperleaf Information assets fall into one of two categories:

- Customer data
- Copperleaf 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 pre-production applications described in section 3.1 are owned and are the responsibility of the Copperleaf customer. In execution of the Copperleaf Services agreement, it is necessary for Copperleaf to process information within these environments, for example when investigating a reported software issue. Copperleaf 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 Copperleaf and its sub-processors. Copperleaf 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 current list of sub-processors involved with the delivery of IFS services including Copperleaf is set out in section 14 (Data Processing).

Copperleaf 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 Copperleaf and any associated data processing terms.

Prior to the termination of a Copperleaf Services agreement, customers may request either the deletion, or offboarding and deletion of data. Copperleaf supports customers with the offboarding process by providing backups of the necessary information assets to help customers restore the information onto an alternative platform. This enables customers to implement, verify and validate their chosen new platform in parallel with the existing environments, and to plan off-boarding and cutover activities to minimize business disruption. The actual technical operational environments are not moved outside the Copperleaf Service due to commercial, legal and technical factors.

At the point of termination of the Copperleaf Services agreement, return of customer data follows a standard process for export and deletion unless otherwise defined within the agreement between Copperleaf and the Customer. Deletion of data from Copperleaf systems, including those hosted in AWS, is in accordance with the recommendations of NIST SP800-88.

Copperleaf Service Operations Data
Copperleaf Service operations data comprises the information associated with the management and operational delivery of the Copperleaf 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 Copperleaf 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 a Copperleaf 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 Copperleaf Services includes comprehensive 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 Copperleaf solutions.

4.1. AWS Access to Copperleaf Services

Employees (and contractors) of Amazon involved with the delivery of AWS cloud services are subject to background checks and monitoring. AWS security design includes the implementation of technical controls preventing staff with physical access to hosting infrastructure also having logical access, and technical controls that prevent AWS staff being able to access Copperleaf data within the hosting environment without Copperleaf active participation. Data secured in services based on the independently verified “Nitro” hypervisor developed by Amazon cannot be intercepted by AWS staff, and Copperleaf uses only services based on this security technology.

4.2. Copperleaf Administrative Access

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

Access to the AWS platforms and infrastructure that make up the Copperleaf Service is not granted to Copperleaf customers.

4.3. Customer Controlled Application Access

Access to Copperleaf Services requires authentication via one of the supported mechanisms described in the Copperleaf Service Description (e.g. single sign-on using the customer’s existing Active Directory). All application-level access is managed by the Copperleaf customer, including user accounts provided to Copperleaf to execute the services defined within the customer’s agreement with Copperleaf (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 Copperleaf Service. The Copperleaf customer can enable and disable such accounts using application administrator accounts provided to them as part of the Copperleaf Service. Certain consulting and support activities included in agreements between Copperleaf and a customer may require Copperleaf administrator accounts to be provisioned by the customer (or by Copperleaf on the customer’s behalf as a component of the activities). It should be recognised that disabling accounts allocated to Copperleaf may prevent delivery of contracted services or fulfilling any applicable service level agreements.

4.4. Monitoring and Threat Detection

IFS Copperleaf Services are monitored for unauthorized intrusions using a combination of network and host-based intrusion detection mechanisms. Copperleaf utilises Rapid7, ESET, and AWS tools

to aggregate logs, provide threat protection using facilities including continuous discovery and monitoring of AWS deployed resources and an assessment of their security status and any applicable security vulnerabilities that need remediation.

AWS monitors network behaviours at the provider level to manage denial of service and control plane attacks, as well as monitoring physical environments for security and other issues.

The Copperleaf team utilise aggregated monitoring and detection tools as part of service monitoring and which are supplemented by further security and health monitoring tools at the application level. Alerts are integrated with Copperleaf Service Management and Incident Management toolsets creating fast, efficient responses to events that require immediate action. Monitoring and detection is an integrated part of Copperleaf's incident management processes – see section 12 below for more details.

4.5. Data Segregation

Copperleaf solutions can, dependant on the product, be fully integrated with the customer's corporate IT network using a secure virtual network, thus adding more security by reducing access directly from the internet.

As shown earlier in this document, the production environment is held separately from the test and demonstration environments in AWS, enabling the deployment of system changes to be properly validated in a secure, safe test environment prior to deployment to production. All Copperleaf 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 Copperleaf Services to help protect information both in transit and at rest.

5.1. Encryption in Transit

All connectivity to Copperleaf Services over the public internet, used for the establishment of the services by the Copperleaf team, includes the use of TLS over HTTPS. 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 protects connections between Copperleaf client systems and AWS cloud services by unique keys. Copperleaf regularly reviews the parameters of TLS configurations and ensures that only cipher suites presently considered appropriate to the security of information are enabled for server connectivity.

Database connectivity internally uses Oracle Native Network Encryption (NNE) using AES-256. Connectivity for customer access to databases and data warehouses can be configured through either Oracle NNE or Oracle TLS at the customer's choice.

Copperleaf services are optionally configured to connect to customer IT domains using an AWS Virtual Private Network (VPN) gateway. 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 AWS. Such site-to-site VPNs use IPsec for transport encryption and requires a customer on-premise VPN device with an external-facing IP address assigned to it.

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 performed within the AWS hosting environment. Data is encrypted using the AES-256 algorithm, utilizing sealed storage for encryption key. Full volume encryption is performed all hosts to protect all data, whether operating environment, application, database, or configuration. Encryption keys and secrets are safeguarded in AWS Key Management Service.

6. Physical & Environmental Security

AWS data centre 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 AWS's Compliance Programs site. AWS are compliant with country or region-specific standards applicable to each region in which AWS data centres are deployed. Rigorous third-party audits verify adherence to the strict security controls which these standards mandate.

6.1. Physical Security Access Controls

AWS data centres used to provide Copperleaf services are designed, built and operated by Amazon in a way that strictly controls physical access to the areas where Copperleaf customer data is stored. Amazon takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the data centre resources. AWS data centres have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the data centre floor.

Amazon does not permit guests or visitors to the AWS hosting facilities. Information on physical security for AWS data center security can be found at AWS's Compliance Programs site.

6.2. Physical Security Reviews

Physical security reviews are conducted periodically of the data centre facilities to ensure that they are running in accordance with the specified requirements. All personnel associated with hosting of the physical data centre do not have logical access to Copperleaf systems within the data centre due to the use of the Nitro hypervisor security architecture.

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 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 the operation of Copperleaf Services.

AWS CloudTrail and CloudWatch are used to gather AWS operational metadata, summarize, and report to central monitoring systems as well as generate alerts directly to security and other tools as needed. Access to AWS monitoring tools is restricted to the cloud operations team with responsibility for platform reliability and engineering.

Application-specific tools are used to collect application and platform logs, and to correlate usage and performance patterns. Access to these logs is restricted to authorized Copperleaf staff responsible for the monitoring of application behaviour.

Security endpoint monitoring is performed with endpoint detection and response, anti-malware, and network monitoring agents, with logs and alerts sent to a central SIEM platform.

7.2. Automation and Templates

Automation tooling is used to automate frequently repeated tasks 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

Copperleaf has implemented application-specific backup solutions to suit standard client requirements, with customized options available for selection. Robust, multi-level backups are performed and replicated in encrypted state to geographically separated storage away from the production environment. Certain aspects of the solution resilience are provided by the AWS services and are built into the service architecture of AWS. 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 centre as well as the secondary, geographically separated data centre where backup/recovery storage is held. Copperleaf customers choose primary and secondary application hosting locations from a list of options at the time of provisioning. Physical separation of data centres utilized by Copperleaf is in accordance with industry best practice 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 to ensure that Copperleaf services can be restored following a major system failure. Recovery in non-disaster events will be to diverse hardware within the primary AWS region, and in disaster scenarios to the secondary AWS region.

The standard retention period for backups is a rolling 90 day period.

7.4. Disaster Recovery

Disaster recovery plans are in place for Copperleaf 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 centre to enable the recovery of the service back to the primary data centre or to a suitable alternative AWS data centre depending upon the nature of the disaster. In the event of a disaster where an entire AWS region becomes unavailable, re-configuration of the customer's connectivity into the service may be necessary and this will be assisted by Copperleaf.

Broader aspects of Disaster Recovery falling outside the scope of Copperleaf 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

Copperleaf Services comprise security logging and monitoring at multiple levels. Amazon Web Services provides logging with associated monitoring at the hardware and infrastructure layer, and alerts and associated remediations are provided by Amazone as part of their service delivery. The

Copperleaf team monitor the health of the Copperleaf Service at platform, application and network connectivity level, generating alerts using various monitoring tools that are reported to the Copperleaf service management system for investigation and actioning as part of Copperleaf Service management.

In additional to service logs and health monitoring provided by Copperleaf, the software provides to the customer capabilities at the application level to log transactional events and utilise these as part of their own internal governance processes.

7.6. Malware Protection and Patching

The Copperleaf Services include the deployment of anti-virus and malware protection services to protect the service components held within the Copperleaf 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 Amazon and Copperleaf according to defined patching and maintenance responsibilities.

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

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

8. Communications

8.1. Customer connections to an IFS Copperleaf Service

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

- Public Internet (with IP whitelisting or geographic filtering)
- VPN (Site to Site)
- AWS inter-tenancy connections

It is important that, whatever connectivity mechanism is chosen by the customer, it is reliable, secure and provides adequate bandwidth and acceptable latency. Selection of the appropriate method is agreed between Copperleaf and the Copperleaf Services customer during on-boarding.

Public Internet Connections

Copperleaf Services can be delivered to customers through the public internet, secured using TLS encryption (HTTPS). IP whitelisting and geographic filters can be implemented where required by the customer to meet data access restrictions and internal policies. This can enable users to access the client from anywhere with an Internet connection, subject to restrictions. This is also compatible with hosted and on-premises access and VPN aggregators with known IP addresses. Public internet access without whitelisting is generally not encouraged for Copperleaf Services, as it exposes the system to the entire internet bringing a broad range of security challenges. If public internet access is required, Copperleaf strongly recommends IP whitelisting be implemented. This blocks access from any location except the customer's nominated IP addresses, providing an important additional layer of security. IP white-listing is implemented and managed as part of the service, but may not be

viable in certain situations - in particular, if the customer's internet connection has a dynamic IP address or if users need to access the system from many unpredictable locations. In those cases, use of geographic filters or VPN aggregators is recommended.

System integrations between Copperleaf Services and other existing Copperleaf customer's IT services are limited when using only public internet access, as the integration mechanisms must be secure. Typically, only HTTPS based integrations (such as web services) are permitted. Integrations based on file transfers, database links, etc are not permitted over the public internet.

Network bandwidth and latency cannot be controlled when accessing over the public internet, and it is important that the customer's internet connection is extremely reliable.

VPN Connections
VPN provides an encrypted tunnel between Copperleaf Services and the customer's own network, effectively making the servers accessible at network level as if they were part of the customer's own internal network. Integrations are possible using VPN, as the secure tunnel provides encryption for integration traffic which would otherwise be unencrypted and insecure. A VPN solution is ideal for creating hybrid cloud solutions where customers need to be able to connect to the Copperleaf solution seamlessly - for example, to integrate with a legacy on-premise system.

The public internet is still used as the network bearer, so bandwidth and latency cannot be controlled, and the customer's internet connection must be extremely reliable. The VPN service requires the customer to provide and manage a compatible endpoint on their network. A list of compatible devices can be provided by Copperleaf as part of service implementation. Any devices supported by AWS for VPN connectivity is generally workable, but Copperleaf are not able to support customers who uses devices that are not included on the supported device list.

Note that only IPsec site-to-site routed VPNs are supported. Layer 2 bridging via VPN is not supported. A network range must be negotiated with Copperleaf for configuration of server IP addresses as network addresses cannot be translated over the VPN.

AWS Inter-tenancy Connections
Amazon Web Services supports publishing Copperleaf services to a customer's AWS account. PrivateLink and DirectConnect are services that allow for AWS to bring customer network traffic to Copperleaf services either from a customer's own AWS services or the customer's remote network.

As with VPN, AWS inter-tenancy connections enable the Copperleaf Services to be accessible at network level as if they were part of the customer's own AWS account or internal network (depending on service and configuration). Connections occur inside AWS without traversing the public Internet. Such connections are more complex and costly than VPN or public Internet connections, but can provide predictable, higher network bandwidth and lower latency. They also add an additional layer of security since the traffic is contained only within a private network, not the public internet.

Non-HTTPS integrations between Copperleaf Services and other customer systems are possible as the connection is encrypted and private.

Copperleaf Services can be linked to an existing customer account if AWS requirements are met. It is the responsibility of the customer to bring network traffic to the inter-tenancy connection, and additional costs for connectivity charged by AWS are the responsibility of the customer.

8.2. Copperleaf's Connection to Customer's Copperleaf Services

The Copperleaf team must connect to the customer's Copperleaf Services in order to implement, monitor, manage and maintain the service. To do this, Copperleaf connects to the customer's

Copperleaf Services using a zero-trust encrypted VPN solution from authorized networks and devices. The Copperleaf management connection is a secure path that requires multi-factor authentication of both the user and the connecting device, and enforces data sovereignty and access restrictions.

Administrative access by Copperleaf staff to the customer's Copperleaf Services via the web application may be restricted by the customer using the user/group/role configurations also used for granting access to customer's own users.

8.3. Internal AWS Communications

Communications between AWS internal components and Copperleaf Services are protected with TLS encryption. Where a service is provided by AWS then the certificates used are signed by Amazon, and where both ends of the connection are Copperleaf services then the certificates used are signed by Amazon or by another certificate provider trusted by the Microsoft Windows operating system for TLS communications.

Copperleaf implements host-specific firewall configurations inside the production network. Several core security and firewall features reside within the AWS-provided environment and which reflect a defence-in-depth strategy. Access to customer Copperleaf Services hosted in AWS is protected by the following layers:

Hypervisor firewall (packet filter): This firewall is implemented in the Nitro hypervisor and configured and reviewed automatically by the Copperleaf deployment and management tool. 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 Copperleaf Services, all traffic is blocked and then the tool adds rules and exceptions in the filter to allow authorized traffic.

Host NIDS agent: The host NIDS agent includes a firewall which protects from malformed and malicious network traffic, inspecting all communications the host receives.

Application configurations: Services are configured to only accept connections from authorized endpoints that provide authentication and meet connection requirements.

9. IFS Copperleaf Service Development & Maintenance

9.1. Security Testing

Product Development Testing
Security testing is performed at multiple stages within the development of Copperleaf Services. Copperleaf products themselves undergo extensive security testing during their development lifecycle within Copperleaf's product development team through automated and manual testing. 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 Copperleaf Services with known vulnerabilities and lack of logging and monitoring facilities.

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

Penetration testing of the Copperleaf Services systems is performed annually by an independent external auditor, and for each release of the software or any substantial change to the environment by an independent internal security team. 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 Copperleaf.

Copperleaf Services customers may request a copy of the penetration tests performed on the same release or version that matches their deployment of Copperleaf Services. The report will be provided under an appropriate non-disclosure agreement only and will be for the customer's information only.

9.2. Vulnerability Management

Copperleaf 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 Copperleaf Services. As described above, known vulnerabilities in AWS infrastructure and platform services and Copperleaf product infrastructure components are patched automatically as part of Copperleaf Services management. Security vulnerabilities identified within Copperleaf products are analysed and security bulletins published on the Copperleaf customer support portal and directly to nominated customer contacts.

Security bulletins will cover vulnerabilities in third party infrastructure components upon which Copperleaf products are built, since these will be important for Copperleaf customers running on-premise solutions. For Copperleaf Services customers, details of how any risk may be mitigated within the Copperleaf Services solution are also included within the bulletin. It should be noted that mitigation actions may differ between Copperleaf Services and on-premise customers depending upon the nature of the specific vulnerability.

10. IFS Secure Product Development Lifecycle

Product development at Copperleaf is conducted by Copperleaf's Product Development team, a component of IFS' Research and Development (R&D) organisation. No outsourcing of development is performed to any third party, and any licensed or open-source dependencies of the product are reviewed before inclusion in the Copperleaf Services.

Copperleaf ensures that all products are developed and supported with consistently high security assurance, and our commitment to continuously innovate in this critical area is a component of our ISMS. Copperleaf's approach to product security includes:

- Code reviews designed to ensure adherence to Copperleaf's development standards;
- Software security testing and code scanning to identify and address security vulnerabilities;
- Release reviews and approvals designed to ensure product releases comply with internal process requirements;
- Vulnerability testing and remediation for infrastructure and tools supporting our product development lifecycle;
- Segregation of product development from other technical environments within Copperleaf, with changes to production application systems undergoing authorization, testing, approval and controlled release and distribution.

Industry standard processes and techniques are used throughout the product development lifecycle including:

- Secure development process and practice,
- Security testing (internal and external),
- Security training and awareness,
- Vulnerability management, metrication and maturity measurement.

Copperleaf customer solutions are established using a formal, controlled release of one of Copperleaf's products to a dedicated deployment environment. Regardless of whether the solution is to be hosted within the customer's own IT environment or within Copperleaf's AWS cloud, the processes used for implementiing and supporting the customer solution preserve the information security throughout. This is achieved using Copperleaf's internal deployment and support tools, formal change management processes, and coordination with customer actvity.

Some customer solutions may involve the use of products developed by Copperleaf partners or involve integrated systems. In such cases, development and support of these products is the responsibility of the partner or integration vendor unless otherwise stated in the Copperleaf agreement with the customer.

11. Information Security & Third Parties

Copperleaf operates 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.

Copperleaf Service are dependent upon very few suppliers for service delivery, the main supplier being Amazon with the provision of the AWS services upon which Copperleaf solutions are hosted. Copperleaf and AWS, as well as all other key suppliers to Copperleaf, operate in close partnership. Supplier management by Copperleaf for key suppliers 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, Copperleaf will notify impacted customers without undue delay of any unauthorized disclosure of their respective customer data by Copperleaf of which Copperleaf becomes aware to the extent permitted by law.

Copperleaf's Incident Management processes have been designed to ensure that forensic information is preserved during the investigation of a security incident and are integrated to IFS's wider incident management processes. Copperleaf 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 Copperleaf Services. Such audits and reviews are conducted by both Copperleaf internal independent audit and review teams and external consultancies and accredited organisations. The

Copperleaf ISMS Management system is reviewed annually by external specialist auditors. This features as part of IFS' commitment to continuous improvement of information security in its products and services. The assessments are conducted in accordance with industry best practice security frameworks including ISO 27001 and AICPA SOC 2.

As part of the ISO 27001 certification of the Copperleaf Service, included within its scope are elements of IFS internal shared services that are subject to internal and external audit, including Information Technology, Human Resource Management and Facilities Management.

As part of Copperleaf's Supplier Management processes, Copperleaf reviews the security credentials of its suppliers, ensuring that they meet Copperleaf 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 supplier's certifications.

13.2. Amazon Web Services Compliance and Certifications

Various audits and certifications apply to the Amazon Web Services platform. Details of compliance can be found in AWS's Compliance Programs site. The following key security and privacy-related audits and certifications for AWS are:

- ISO27001 – Information Security Management
- ISO27017 – Cloud Security Controls
- ISO27018 – Personal Data Protection
- SOC 1, 2, and 3 – System and Organization Controls Reports
- Cloud Security Alliance (CSA) STAR Certification

13.3. Exclusions

IFS Products, including Copperleaf Services, by their nature can be used for many different business purposes. Some of these relate to regulated industries requiring particular certifications. IFS and Copperleaf do not certify their 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 Copperleaf 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	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	Control Measures	Country
Copperleaf Technologies, Inc		Copperleaf SaaS	Cloud Services, Support, R&D Product Support	Measures described in this document. Intragroup Agreement including SCCs	Canada
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	Control Measures	Country
Amazon Web Services	Cloud platform services	Cloud Service Provision	AWS DPA AWS Nitro Hypervisor AWS Key Management Service	Data centre location will be specified in the contract with customer or selected as part of on-boarding

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

None

14.4. Data Processing Descriptions

Project Implementation

In order to support the customer with the implementation of a Copperleaf solution, Copperleaf performs a range of activities, each of which may result in the processing of customer data. Such activities are performed by the Copperleaf consulting team for the region in which the solution is to be implemented and may involve the support of other regional consulting teams and Copperleaf staff. Copperleaf regional and global support teams may also be involved in the implementation phase in resolving any product defects identified during the implementation. Copperleaf follows 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 Copperleaf support agreement, Copperleaf support teams may require access to customer production or reference environments containing customer production data in order to investigate reported software issues associated with the Copperleaf product. The investigation of certain product issues may require the involvement of Copperleaf Product Development.

Copperleaf Cloud Services

Where Copperleaf customers choose the Copperleaf Cloud service, their Copperleaf products that form their solution are hosted in Amazon Web Services data centres. Selection of the datacentres is part of on-boarding.

Copperleaf consulting and support teams access the customer environment in AWS 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 AWS platform upon which the customer's solution will run;
- Installation of the Copperleaf 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.

The Copperleaf cloud operations 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 AWS platform and the associated Copperleaf products.

AWS Service Provision
AWS data centers are managed and maintained by Amazon in accordance with their ISO 27001 and SOC 2/SOC 3 certified processes. Their responsibilities are to ensure the AWS services utilized by Copperleaf solutions remain available and performing in accordance with their specification. The AWS services consumed by the Copperleaf cloud solutions include:

- Infrastructure as a Service (IaaS) processing, storage, site recovery and network services
- Platform as a Service (PaaS) databases

Amazon do not have access to applications within the virtualized environments within which the Copperleaf products that make up our customer solutions run nor underlying data secured via the Nitro hypervisor. They therefore do not have access to customer production data held within Copperleaf cloud solutions. Amazon's processes for managing the AWS data centers employ segregation of duty principles and technical controls to prevent access to customer data.

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, India and Poland. Corporate Services do not process customer data, instead they implement and maintain the internal IT services and equipment that support the IFS business operations, including those of Copperleaf. Whilst this includes the use of administrative level accounts, it does not include access to customer solution platforms and accounts.

Document Revision History

Rev.	Date	Owner	Remarks
1	21/03/2025	Ricard Kelly	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