# IFS Information Security

A firm commitment to information security runs throughout IFS. It's present in each employee and each member of the IFS Board. We're dedicated to safeguarding the information of our customers, partners, suppliers and staff, and this reflects in the tools and processes we maintain and operate every day.

Our Information Security Management System (ISMS) is based on ISO 27001, bringing it in line with international best practice. The ISMS comprises all our information security policies, processes and guidelines and is reviewed frequently to make sure we're steps ahead of the latest security threats.

## Ensuring a security-conscious workforce

Every day we are committed to delivering the best possible service to 10,000+ customers across the globe. Paramount to this is ensuring our 4,000 strong workforce treat company and customer information responsibly during their time at IFS–and after they leave.

To keep internal and external information secure, we:

- Conduct thorough background checks on new hires–both full-time employees and fixed term contractors.
- Deliver information security and data privacy training, as part of the staff induction process. Refresher courses are conducted annually.
- Restrict employee access to information and systems according to job role and the principles of "need to know" and minimization. Each employee user account is auditable.
- Operate a formal off-boarding process when an employee leaves the company. The person is reminded that the confidentiality agreement they signed when joining IFS persists beyond their employment. We ensure all company equipment is returned and all system access revoked.

## Key facts

At IFS, we apply best practice to:

- **Our people**–through vetting and education before, during and after their employment
- **Access control**–via multi-factor authentication, fully auditable user accounts and more
- **Data encryption**–with sophisticated protection of data in transit and at rest
- **Physical security**–through modern, secure data centers and employee offices
- **Malware protection**–with robust, proactive tools and techniques
- **Security testing**–via frequent vulnerability scanning and penetration testing
- **Network security**–with a dedicated, specialist team managing our Security Operations Centre 24x7
- **Third-party security**–by applying strict codes of conduct to all our suppliers and partners
- **Business continuity**–via frequent testing and refinement of our disaster recovery and crisis management procedures

## Controlled access to customer environments

**At IFS, we apply rigorous access controls including:**

- Multi-factor authentication–for accessing IFS and customer environments from remote locations. We use a wide range of security measures, including physical security controls, trusted asset certification, trusted network access and second factor user authentication.
- IFS SupportNet–a secure connection method using industry best practice protocols. We perform regular penetration testing on it, enabling us to securely connect to the customer's production system and deliver services that are part of the customer's IFS Agreement.
- Shared user accounts–these are needed fwor accessing customer environments and delivering our services but are attributable to individual IFS users. Therefore, such account usage is fully traceable and auditable. Access to shared accounts and associated passwords is restricted on a "need to know" basis and customers can control access to their solutions through the management of the user accounts.

## Data encryption across all devices

Data is encrypted where necessary, for example when storing highly sensitive or confidential information on mobile devices and laptops or when accessing IFS environments from remote working locations. For data at rest, we use certified encryption protection if the information is sensitive or at risk of loss. For example, FIPS 140-2 L3 (a U.S. government computer security standard) on removable media may be used in such cases.

For data in transit, we apply protection such as site-to-site VPN connections and point-to-site VPN connections. We employ Certificate Authorities to manage public keys rather than self-signed certificates and manage encryption keys centrally, as corporate assets.

## Consistent physical security controls across the globe

Our internal global IT systems and services are hosted in three external, professionally managed colocation data centers. Based in Sweden, USA and Sri Lanka, all centers employ resilience and redundancy to ensure continued availability of service. Staff access is limited to a small number of individuals and access logs are regularly audited.

**IFS have office locations in over 30 countries across the world. Each site employs combinations of the following according to the local environment and applicable laws/ regulations and IFS's own risk assessments:**

- A security-driven layout–for example, the risk of unauthorized individuals overlooking sensitive information, through windows or meeting room glass panels, is factored into the design of the office
- CCTV, user identity badges and swipe card access
- Restricted access locations and secure archiving facilities
- Clear screen and clear desk policies

## Robust, proactive malware protection

To fully secure our customers' data, we've deployed enterprise-grade malware protection across our entire end user population and server infrastructure. Virus signature updates are applied automatically at regular intervals. Software patching of all managed server and client operating systems is performed centrally using automated deployment tools. This ensures critical security patches of operating systems and software products deploy consistently and on time.

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

- Store backups securely, protecting them against ransomware attacks and encrypting them to protect confidentiality.
- Manage backup retention to ensure that data recovery objectives can be fully satisfied and that secure destruction takes place when they are no longer required.
- Test restoration processes quarterly. We do this by refreshing test environments from live production environments (and obfuscate sensitive data in the process).

## Continuous improvement through regular testing

Our cybersecurity teams and technology never stand still. To get ahead of the latest threats, we perform frequent vulnerability scanning, adapting business systems and environments where needed. And as with any strong security program, these activities never exist in a vacuum—external specialists regularly perform extensive penetration testing of our IT systems and networks.

Moreover, we frequently invite specialist organizations to review our Information Security Management System processes, as part of our commitment to continuous improvement.

## 24/7 network security

At IFS, we're continually honing our ability to detect security incidents through continual monitoring and analysis of system, network and user activity. Our 24/7 Security Operations Center (SOC) team use a combination of traditional and AI-based tools to monitor, detect and remediate security events on the IFS network.

The SOC team are equipped to quickly isolate and resolve any suspicious activity on the network, including attempted data exfiltration to external unauthorized destinations.

## Fortifying the supply chain

To safeguard our customers' data, the evaluation of our own systems, infrastructure and people should only ever be part of the picture. Cyber criminals rarely enter through the front door—in fact, according to research, up to 80% of cyberattacks now begin in the supply chain. To successfully deal with this risk, and achieve tight third-party security, we ensure all our suppliers agree to our strict global code of conduct. To protect confidentiality, our suppliers are bound to non-disclosure agreements, as well as data processing and data transfer agreements, where necessary.

IFS suppliers are required to adhere to the relevant aspects of the IFS information security incident management process. We audit suppliers' security practices and monitor their performance, in accordance with information security arrangements, for the entirety of the contract.

## Ensuring business continuity

Our disaster recovery and crisis management processes are ready and waiting, should disaster ever strike. Part of our Business Continuity Management System (BCMS), these processes help ensure we can continue to deliver our services in such an event.

Through the development of crisis management playbooks and prescribed roles and responsibilities, our team are prepared to tackle the full range of scenarios—from utility disruptions and cyber attacks through to flooding, earthquakes and other forms of natural disaster. Through a combination of desk and scenario-based exercises, we road test the BCMS at regular intervals to ensure it remains as robust and responsive as possible.

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. 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.

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

IFS

Production: IFS, September 2021