Information Security

Requirement for Third Party Suppliers

IFS Ultimo

Contents

1. Introduction 3
2. Information Security Management 3
3. Roles & Responsibilities 3
4. Definition of Terms 3
5. Acceptable Use 4
6. Information Security Policy 4
7. Organisation of Information Security 5
8. Human Resources Security 5
9. Asset Management 5
10. Access Control 6
11. Physical and Environmental Security 7
12. Operations Management and Communications Security 8
13. Information Systems Acquisition, Development and Maintenance 10
14. Risk Management 11
15. Information Security Incident Management 11
16. Resilience 11
17. Compliance 12
Review & Amendment 12
Confirmation 12

1. Introduction

As part of IFS Ultimo's commitment to information security, it is essential that all those who support IFS Ultimo through the provision of products and services apply their own information security controls in accordance with Good Industry Practice. The information security standards set out in this document are aligned with the international recognized ISO27001 framework and represent the minimum expected security baseline to be applied by the Third Party Supplier when providing such products and/or services.

The focus of the requirements below is to support compliance, rather than how compliance must be met, this is to allow for greater flexibility within Third Party Suppliers to determine how best to comply, through their own information security policies and processes.

Where Third Party Suppliers are required to access IFS Ultimo information systems in connection with the fulfilment of their supplier agreement, alternative requirements contained in the "*IFS Ultimo Information Security Requirements for Third Party Suppliers Using IFS Ultimo Information Systems"* policy will apply.

2. Information Security Management

All contracts with Third Party Suppliers must have the "IFS Ultimo Information Security Standards for Suppliers" (this document) appended to them and which defines the Information Security obligations applicable.

3. Roles & Responsibilities

All third party agreements are handled with support from the Legal and Security teams. From time to time, IFS Ultimo may update its Information Security Standards for Suppliers documentation and in such cases, IFS Ultimo will update Third Party Suppliers accordingly. Third Party Suppliers are responsible for complying with IFS Ultimo Information Security Standards for Suppliers and must engage with IFS Ultimo to confirm their interpretation or obtain further information where necessary.

4. Definition of Terms

IFS Ultimo Information Security Standards for Suppliers – This document.

Information Security Obligations – The obligation for a Third Party Supplier to comply with the IFS Ultimo Information Security Standards for Suppliers documentation and any other security requirements contained within the contract including, but not limited to, NDAs and GDPR considerations.

Third Party Supplier – Any company or organization that provides IFS Ultimo with a tangible product, support, consultancy or solution, either directly or indirectly through a sub-contractor.

Good Industry Practice – Standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector.

IFS Ultimo Information –Data provided by, owned by, processed by or developed by IFS Ultimo, including intellectual property (IP), personally identifiable information (PII) regarding IFS Ultimo employees or that of its customers, partners or other suppliers.

Contracted Service –The commercial agreement between IFS Ultimo and the Third Party Supplier as defined in an agreement or Statement of Work (SoW).

Sensitive Information – Any information created, collected or used by IFS Ultimo and/or an IFS Ultimo Customer in the conduct of its business including, but not limited to:
• the employment of its employees;
• collaboration with its partners;
• execution of customer contracts;
• to manage key financial aspects of the business.

Confidential Information – Personally Identifiable Information (PII) protected by data protection laws and regulations in order to safeguard the privacy interests of the data subject.

5. Acceptable Use

Objective: To ensure that the Third Party Supplier end users understand their information security responsibilities to protect IFS Ultimo Information.

1. Third Party Suppliers must comply with the information security requirements set out in this document.
2. Third Party Suppliers handling IFS Ultimo data must as a minimum, ensure their end users comply with the following:
    a. Handle IFS Ultimo Information in accordance with its classification, not sharing it with other third parties, and only processing it as necessary to deliver the Contracted Services;
    b. Never post or discuss IFS Ultimo Information on public forums such as social media or networking sites.
    c. Keep IFS Ultimo Information secure at all times, utilizing Good Industry Practice to prevent it being accessed by unauthorized users;
    d. Be aware of who may be listening when discussing IFS Ultimo Information;
    e. Securely dispose of IFS Ultimo Information in accordance with secure disposal processes including secure physical and electronic disposal in accordance with Good Industry Practice.

6. Information Security Policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

1. Third party suppliers must have an Information Security Policy and associated set of processes which must:
    a. Align with Good Industry Practice;
    b. Be approved by senior management within the Third Party Supplier organization;
    c. Be published and communicated to all Third Party Supplier employees and contractors;
    d. Take into account legal and regulatory requirements and Information Security Obligations.
2. Third Party Suppliers must review their Information Security Policies at least annually and have them approved by senior management to ensure its continuing suitability, adequacy and effectiveness.
3. Third Party Suppliers must define and implement processes and procedures to support their Information Security Policies and ensure their compliance with these Information Security Obligations.
4. Third Party Suppliers must review the supporting security processes and procedures at least annually to ensure their continuing suitability, adequacy, and effectiveness and ensure awareness within the business.

7. Organization of Information Security

Objective: To establish a management framework to initiate and control the implementation of information security within the Third Party Supplier's organization.

1. Third Party Suppliers must appoint individual(s) with authority to implement their Information Security Policies and who are accountable for complying with these Information Security Obligations.
2. Information security responsibilities must be clearly defined within the Third Party Supplier's organization and specific activities required to support the Information Security Policies and these Information Security Obligations must be allocated to the appointed individual(s).
3. Information security activities coordinated within the Third Party Supplier's organization must cover the part of its business providing the Contracted Service to IFS Ultimo.

8. Human Resources Security

Objective: To create and maintain a security aware culture, where third party users understand the value of information security and act according to their individual responsibilities.

1. Third Party Suppliers shall ensure that pre-employment screening is completed for the Third Party Supplier's employees and contractors before they support the delivery of the IFS Ultimo Contracted Service
2. Third Party Supplier line management must brief users on their information security responsibilities before being involved with the delivery of IFS Ultimo Contracted Services. Third Party Suppliers must develop, implement, maintain and monitor information security awareness and provide training for Third Party Supplier users and sub-contractors, on a regular basis.
3. Third Party Suppliers must define and implement processes for secure and timely management of Starters/Changes/Leavers so as to reduce any security risks, these activities must include:
    a. Account cessation no later than the final working day of a Leaver;
    b. Timely retrieval of IT assets from a Leaver;
    c. In the event of a change of role, a full review of access rights must be conducted;
    d. Retain evidence that these processes have been followed.

9. Asset Management

Objective: To identify organizational assets and define appropriate protection for Third Party Suppliers information and IT Systems.

1. Third Party Suppliers must dispose of, or provide services to enable IFS Ultimo to dispose of, any IFS Ultimo sensitive or confidential information they hold in a suitably secure manner to prevent data recovery upon completion of any contractual agreement.
2. Third Party Supplier IT Systems must be suitably protected against compromise and governed by the Third Party Suppliers information security framework.
3. Third Party Supplier IT Systems which store, process or have access to IFS Ultimo Information must be recorded in information asset inventories along with their ownership, classification and location details.
4. Third Party Supplier must operate asset management in such a way that IT assets are assigned to individuals and security wiped prior to transfer or repurposing.

10. Access Control

Objective: To limit access to information and information processing facilities on a "need to know" basis.

1. Third Party Suppliers must define, implement and maintain an access control policy and supporting technical standards which should include:
    a. Business and security requirements for access;
    b. Least privilege principle, and security levels;
    c. Classification of information;
    d. Segregation of access control roles.
2. Third Party Suppliers must define, implement and maintain formal user registration and de-registration procedures for granting and revoking access to information assets.
3. Third Party Supplier's user access controls must:
    a. Assign a unique user identifier to each third party user;
    b. Not display or store passwords in clear text during user login;
    c. Authenticate the user before access is provided;
    d. Not display error or help messages that would facilitate an unauthorized access attempt;
    e. Lock the user's screen after no more than 15 minutes of inactivity and force revalidation;
    f. Force passwords to be changed if they have been set by administrators;
4. Third Party Suppliers must control the allocation of passwords through a formal management process and Third Party Supplier's user passwords must:
    a. Be updated only when the user has been authenticated;
    b. Not be stored or transmitted in clear text in Third Party Supplier IT Systems;
    c. Be protected from unauthorized access and change;
    d. Be distributed only to the user who owns the account (or an approved alternate user);
    e. Be used only by the user who owns the account.
    f. Passwords for Third Party Supplier IT Systems must:
    g. Be technically enforced;
    h. Be at least eight characters;
    i. Be different from their associated unique identifier;
    j. Be subject to change on first login, if provided by an administrator;
    k. Contain characters from at least three of the following:
        i. numbers;
        ii. upper case letters;
        iii. lower case letters;
        iv. special characters (e.g. &^%).
5. Third Party Suppliers must not permit the use of shared accounts whose use cannot be traced back to a named user.
6. Third Party Suppliers must restrict and control the allocation and use of system and privileged accounts by:
    a. Allocating on a need-to-use basis or on a per task basis in line with the Third Party Supplier access control policy;
    b. Using an authorization process and maintaining an inventory of all system and privileged accounts allocated;
    c. Permitting generic accounts if they are attributable to an individual.
7. Third party Supplier user entitlement reviews must:
    a. Be conducted at least annually for Third Party Supplier IT Systems;
    b. Be conducted using a segregation of duties principle;
    c. Must be conducted by an accountable person;
    d. Must be recorded.
8. Third Party Suppliers must have a policy and procedures for remote-working activities. Remote access to Third Party Supplier IT Systems must:

   a. Meet the requirements of the Third Party Supplier's own user access control policy;
   b. Be approved and documented;
   c. Use multi-factor authentication where accessed across a public network;
   d. Prevent local storage of IFS Ultimo Information on non-Third Party Supplier devices;
   e. Use appropriate encryption to protect IFS Ultimo Information transmitted over public networks.
9. Third Party Suppliers must ensure that sub-contractors accessing Third Party Supplier IT Systems:
   a. Comply with the minimum IT security requirements set out in this document;
   b. Comply with the requirements of the Third Party Supplier's user access controls;
   c. Have their access reviewed in accordance with user entitlement reviews;
   d. Access the Third Party Supplier IT Systems only for approved time periods;
   e. Have an agreed and active contract and non-disclosure agreement in place before access is provided;
   f. Use connection methods approved by the Third Party Supplier;
   g. Are subject to Third Party Supplier security reviews to verify that sub-contractors are handling and storing IFS Ultimo Information securely and in accordance with the Information Security Obligations.
10. Third Party Suppliers must restrict, control and monitor the use of utility programs tools.
11. Where applicable, Third Party Suppliers must have a personal device policy for such devices that connect to the Third Party's business system that:
   a. Permits the device to be remotely wiped or confiscated;
   b. Contains security measures to protect against the risks of using mobile computing and communication.

11. Physical and Environmental Security

Objective: To protect IFS Ultimo Information and IT Systems and supporting Third Party Supplier IT Systems from unauthorized physical access, disruption and malicious attacks.

1. Access to Third Party Supplier IT Systems and data centers or information storage facilities used in the provision of the Contracted Service, must be:
   a. Restricted to authorized individuals or to escorted visitors;
   b. Monitored, recorded and access records retained.
2. Third Party Supplier IT Systems, data centers and/or information storage facilities used in the provision of Contracted Service must be designed to:
   a. Protect Third Party Supplier IT Systems or sub-contracted IT Systems from natural disaster;
   b. Provide lockable server racks for Third Party Supplier IT Systems;
   c. Protect power cables from communications cables from interference;
   d. Manage the temperature and humidity in accordance with equipment manufacturer recommendations;
   e. Protect the physical security perimeter from unauthorized access, damage, and threats;
   f. Provide resilience;
3. Third Party Supplier IT Systems must:
   a. Be maintained in accordance with the manufacturer's recommended service intervals and specifications;
   b. Record suspected and actual faults;
   c. Record any related remedial action taken regarding the applicable fault.
4. Before the disposal or repurpose of any Third Party Supplier IT Systems, any IFS Ultimo Information held on such systems must be securely erased, ensuring there is no possibility of the data being recovered.
5. Obsolete Third Party Supplier IT Systems used to store or process IFS Ultimo Information classified as Sensitive must:

   a. Not be transferred or sold to a third party without being securely wiped;
   b. Be securely disposed of by physical destruction if at end of life;
   c. The Third Party Supplier shall keep documented certification of the secure disposal and be able to provide to IFS Ultimo on request.
6. Holding or storage areas, where Third Party Supplier IT Systems containing IFS Ultimo Information is held before the destruction or secure erasure, must be protected against unauthorized access.

12. Operations Management and Communications Security

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

1. Operational procedures for managing Third Party Supplier IT Systems used to access, manage, store or process IFS Ultimo Information or access IFS Ultimo IT Systems, must be documented, maintained, and made available to all users who require them. As a minimum, the operational procedures must cover:
   a. Change, configuration and release management;
   b. Capacity management;
   c. Technical vulnerability and patch management;
   d. Network management.
2. Third Party Suppliers must develop and implement a policy on the use of cryptographic controls for protection of information in accordance with their Information Security Policy, legal requirements, regulatory requirements and these Information Security Obligations.
3. Key management must be in place to support the Third Party Supplier's use of cryptographic techniques.
4. Third Party Supplier's IT Systems used to store, process or access IFS Ultimo Information classified as Sensitive must protect against information loss by:
   a. Identifying potential data loss channels;
   b. Implementing data loss protection solutions and procedures to cover data loss channels identified in accordance with point a);
   c. Detecting IFS Ultimo Information disclosed to unauthorized parties;
   d. Handling any actual or suspected data loss incidents in accordance legislation, regulation and informing IFS Ultimo without undue delay and within 48 hours of the incident;
5. Third Party Suppliers must obtain timely information about technical vulnerabilities of Third Party Supplier IT Systems, evaluate the Third Party Supplier's exposure to such vulnerabilities, and take appropriate measures to address the associated risk. Technical vulnerability management must be implemented in an effective, systematic, and repeatable way with measurements, consistent with Good Industry Practice.
6. Third Party Suppliers must segregate development, test, and operational facilities to reduce the risks of unauthorized access or changes to the operational Third Party Supplier IT Systems.
7. Third Party Suppliers must take and test regularly systems backups, in accordance with a backup policy which shall be maintained in accordance with Good Industry Practice.
8. The Third Party Supplier's IT network topology must be documented and maintained with sufficient detail to manage the IT network effectively and securely.
9. Third Party Supplier IT networks must be managed and controlled in a way so as to ensure that they are protected from common threats in line with Good Industry Practice.
10. Third Party Supplier IT networks used in the provision of the Contracted Service and which are accessed from an external connection, outside of those IT networks, must:
    a. Be monitored for suspicious and malicious activity;
    b. Restrict external network traffic only to authorized parts of the IT network;
    c. Restrict connections to defined entry points;
    d. Limit available protocols to the minimum required to perform the required role.

11. Inbound connections to the Third Party Supplier IT network must be suitably protected against unauthorized access using as a minimum, strong passwords and account lockouts after a small number of incorrect attempts.
12. Configurations and rule sets used on devices with firewall functionality must be:
    a. Verified to confirm that rules are valid and that expired, duplicate or unnecessary rules have been removed;
    b. Restricted to authorized users;
    c. Managed and updated in line with the manufacturer's recommendations.
13. Externally facing web applications must be:
    a. Protected by an application, firewall or a device with equivalent functionality and by implementing measures and controls that identify and protect against unauthorized access and disruption.
    b. Penetration tested and venerability scanned at least annually.
14. Third Party Suppliers must implement intrusion detection or prevention solutions which must:
    a. Be protected against unauthorized attack or change;
    b. Be configured to alert the Third Party Supplier when unauthorized and suspicious activity is detected;
    c. Analyze suspected intrusions;
    d. Be automatically updated to identify and respond to new attacks.
15. To protect IFS Ultimo Information on removable media, Third Party Suppliers must:
    a. Encrypt IFS Ultimo Information stored on removable media.
    b. Require a strong password to protect Sensitive IFS Ultimo Information.
    c. Require secure disposal when no longer required, using validated procedures in line with Good Industry Practice.
16. Third Party Suppliers must protect laptops which are used to access, manage, store or process IFS Ultimo Information using cryptographic algorithms and techniques that meet Good Industry Practice.
17. Third Party Suppliers IT System documentation and information associated with the interconnection of Third Party Supplier IT Systems must be protected against unauthorized access.
18. Third Party Suppliers must implement policies, procedures, and controls to protect the exchange of information through the use of all types of communication facilities including electronic messaging.
19. Third Party Suppliers must protect media containing IFS Ultimo Information from unauthorized access, loss, misuse or corruption during transportation beyond their physical or logical boundaries.
20. Third Party Suppliers must protect the integrity of IFS Ultimo Information when hosted on Third Party Supplier IT Systems available to the public, on behalf of IFS Ultimo.
21. Systems clocks must be synchronized with an accurate NTP time source and protected from tampering.
22. Third Party Suppliers must define and implement procedures for monitoring Third Party Supplier IT Systems and regularly reviewing the results of the monitoring activities.
23. Third Party Suppliers must produce audit logs recording user activities, system administrator and system operator activities, exceptions, and information security events and retain these logs for appropriate period to assist in incident investigations and access control monitoring.
24. Third Party Suppliers must protect logging facilities and log information, from tampering and unauthorized access.
25. Logs must not contain user passwords or sensitive Personal Identifiable Information.
26. Logging and monitoring should be conducted by authorized individuals on Third Party Supplier IT Systems.
27. Third Party Suppliers must monitor the following Information Security Events:
    a. Unauthorized access and unsuccessful access attempts;
    b. The creation, modification and use of privileged user accounts;
    c. Third party access to IFS Ultimo Information classified as Sensitive;

d. Unauthorized device connection to the IT network;
e. Alerts from network gateways and firewalls;
f. Alerts from intrusion detection and prevention systems.

13. Information Systems Acquisition, Development and Maintenance

Objective: To protect Third Party Supplier IT Systems by consistently implementing information security requirements at each stage of the systems development lifecycle.

1. Third Party Suppliers must implement a documented systems development lifecycle process which evidences security at every stage.
2. Development, test and user acceptance testing activities must be segregated from production activities to protect the production environment.
3. Third Party Suppliers must risk assess the use of open source software in Third Party Supplier IT Systems before implementation.
4. Third Party Suppliers must restrict and control access to program source code to prevent the introduction of unauthorized functionality and to avoid unintentional changes.
5. Third Party Suppliers must perform technical vulnerability tests in accordance with the following requirements:
   a. At least quarterly on Third Party Supplier IT Systems storing or processing IFS Ultimo Information;
   b. At least quarterly for application technical vulnerabilities on Third Party;
   c. Supplier web-based applications storing or processing IFS Ultimo Information;
   d. Vulnerability tests shall be carried out by a reputable scanning tool.
6. Third Party Suppliers must perform penetration tests on externally facing Third Party Supplier IT Systems or web-based application(s) which handle Sensitive information on Third Party Supplier IT Systems that store, process and transmit IFS Ultimo Information at least annually and on material change.
7. Third Party Suppliers must implement a documented change management process which requires that:
   a. Changes have an information security business impact assessment performed;
   b. Changes are formally documented in a change request and approved by authorized users;
   c. Segregation of duties is in place for the requesting, authorizing and implementation of a change;
   d. A ‘recover position’ is defined, so that Third Party Supplier IT Systems can recover from failed changes or unexpected results; and changes are verified.
8. Third Party Suppliers must develop, implement and maintain a process for applying emergency fixes to Third Party Supplier IT Systems used in the provision of the Contracted Service.
9. Third Party Suppliers must implement a documented software release management process which requires that releases are subject to change and version control.
10. Third Party Suppliers IT Systems must be subject to appropriate capacity management to prevent degradation of performance.
11. Third Party Suppliers must implement detection, prevention, and recovery controls to protect against malware.
12. Test data must be selected in accordance with Good Industry Practice and protected and controlled.
13. Third Party Suppliers must have processes to:
    a. Sanitize data used for testing to remove sensitive data such as IP and PII;
    b. Protect the integrity of production data;
    c. Remove test data from the environment post testing.

14. Risk Management

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

1. Third party suppliers must establish and manage a documented ISMS, covering the Contracted Service within the contracted scope.
2. Third party suppliers must establish an information security risk framework which includes:
   a. Implementing a risk assessment methodology.
   b. Periodically analyzing and evaluating the risks.
   c. Risk acceptance criteria.
   d. Risk treatment plans.
   e. Periodic review with senior management.
3. Before using a sub-contractor for Contracted Service activities, Third Party Suppliers must ensure that the sub-contractor meets the standards set out in this document.

15. Information Security Incident Management

Objective: To minimize the business impact of information security incidents and to reduce the risk of similar incidents occurring.

1. Third Party Suppliers must define, implement and maintain information Security incident reporting processes.
2. Third Party Suppliers must at least annually test that information security incident reporting channels.
3. Third Party Supplier shall ensure that their employees and sub-contractors report to the IFS Ultimo any actual or suspected information security events related to the Contracted Service:
   a. As soon as it is practical, but no later than 48hrs after the incident.
   b. Through defined information security incident reporting processes developed by the Third Party.
4. Third Party Suppliers response to information security incidents must include:
   a. Containing and resolving the incident;
   b. Recording all incident response activities;
   c. Performing a root cause analysis;
   d. Implement preventative measures;
   e. Supporting IFS Ultimo if materially affected.
5. When forensic analysis and investigation is required on Third Party Supplier or subcontracted IT Systems which store, process or access IFS Ultimo Information, it must be undertaken by suitably trained people or third parties.
6. The integrity of evidence must be protected by the Third Party Suppliers during forensic analysis and investigation by:
   a. Taking steps to protect the environment, within which the analysis and investigation is being carried out, and initiate the chain of custody;
   b. Maintaining the chain of custody for collected evidence and exhibits;
   c. Preventing and detecting any tampering of evidence;
   d. Avoiding contamination, by analyzing evidence in a controlled environment.

16. Resilience

Objective: To maintain IT system availability in accordance with Contracted Service level agreements and minimize the risk of IT system failure.

1. For Third Party Supplier IT Systems, Third Party Suppliers must:
   a. Minimize potential single points of failure;
   b. Use fault tolerant architecture;
   c. Manage capacity;
   d. Apply standard maintenance practices;
   e. Manage and maintain appropriate backups;

f. Implement business continuity measures.

17. Compliance

Objective: To avoid breaches of any law, statute, regulation or contractual obligations and of any security requirements.

1. Third Party Suppliers must identify, interpret and address the information security implications of relevant legislations and regulations applicable to the Contracted Service.
2. Third Party Suppliers must implement mitigating controls where national or international regulatory or contractual constraints restrict the use of cryptographic solutions. Mitigating controls must be applied where cryptography cannot be used.

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 Ultimo change management processes.

Confirmation

By signing this policy, Third Party supplier confirms to have read and familiarised chain partner self with the above and commit to adhering to the principles and requirements.

Company name:

Name of person authorised to sign:

Position:

City:

Date:

☐ I hereby confirm that I have read and understood this policy.