Information Security

Standards for Third Party Suppliers Using IFS Ultimo Information Systems

IFS Ultimo

Contents

1. Introduction

As part of IFS Ultimo's commitment to information security it is essential that all those who have access to (Sensitive) Information Systems belonging to IFS Ultimo or IFS Ultimo Customers are aware of their obligations to adhere to our information security policies, standards and practices. This document describes these obligations which are mandatory for End Users who have been given access to IFS Ultimo Information Systems and/or IFS Ultimo Customer Information Systems in order to provide a service or product to IFS Ultimo and fulfil their responsibilities.
Failure by the End User to meet these obligations may involve criminal liability and/or exclusion from IFS Ultimo/Customer Information Systems, projects and contracts.

2. Definition of terms

For the purpose of this document the following terms have been defined and used throughout:

Sensitive Information – Any information created, collected or used by IFS Ultimo and/or an IFS Ultimo Customer that is not intended for general public disclosure, but which is made available as necessary in order to support IFS Ultimo and/or a Third Party Supplier to deliver its products and services in accordance with a formal agreement.

Including:
– 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.

– Personally Identifiabe Information (PII) protected by data protection laws and regulations in order to safeguard the privacy interests of the data subject.
I
Information Systems – Comprises both electronic and hardcopy systems which capture, store and process Sensitive Information and includes, but is not limited to, software applications, IT services, IT networks, filing systems, email servers, etc.

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

Contracted Service –The commercial agreement between IFS Ultimo and the Third Party Supplier as defined in a contract or statement of work (SoW).

End User –Employed by a Third Party Supplier under any form of agreement to perform activities or deliver services on behalf of the Third Party Supplier and who requires access to IFS Ultimo or IFS Ultimo Customer Information Systems in order to perform their duties.

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.

3. Information Security Responsibilities

1. IFS Ultimo is responsible for maintaining the information security policies, standards, processes and procedures applicable to its Information Systems so as to:
    a. Protect IFS Ultimo, employee, customer, partner and supplier information held by IFS Ultimo against any unauthorised access;
    b. Preserve the confidentiality, integrity and availability of such information;
    c. Satisfy legislative and regulatory requirements in all countries within which IFS Ultimo operates.
2. By providing Third Party Supplier with access to IFS Ultimo' Information Systems, they accept the following obligations:
    a. Compliance with the IFS Ultimo security and personal data processing requirements included in this document;
    b. With regard to IFS Ultimo and/or IFS Ultimo customer data, an undertaking not to use the information, either directly or indirectly, for any purpose other than to carry out the agreed Contracted Service.
    c. Compliance with IFS Ultimo' instructions as communicated at any time for handling personal data and any other security provisions;
    d. Failure to comply with the requirements of this document may result in the removal of access to IFS Ultimo' Information Systems/services.
3. By submitting information to IFS Ultimo, the Third Party Supplier is solely responsible for the submitted information and is responsible for their own actions and consequences of submitting information in accordance with applicable laws and regulations, including, but not limited to, information in violation of the above mentioned laws and regulations and information in violation of competition laws and regulations and copyright legislation. By accepting these terms the Third Party Supplier confirms and warrants that they have the consent, authority and permission to submit the information.
4. The Third Party Supplier shall be responsible for ensuring that their End Users are aware of their responsibilities as defined within this document and act in accordance with them.

4. Information Security Responsibilities

1. A Master Service or Non-disclosure agreement shall exist between IFS Ultimo and the Third Party Supplier to protect both party's interest and under which the End User is obligated.
2. The entire right, title and interest in the IFS Ultimo information made available to the End User/Third Party Supplier through IFS Ultimo Information Systems shall remain with IFS Ultimo. The End User/Third Party Supplier shall not have any right to this information apart from what is stipulated in this document or IFS Ultimo license.
3. The collection of any Sensitive Information regarding the Third Party Supplier and/or their End Users by IFS Ultimo shall be with their approval.
4. All information, either in hardcopy or electronic form, that is created, stored or processed by the End User and belonging to IFS Ultimo or an IFS Ultimo Customer shall be managed in accordance with:
    a. Its sensitivity so as to protect its integrity, confidentiality and availability;
    b. Applicable data privacy and protection legislation and regulations under which it is governed.
5. The Third Party Supplier shall minimise the volume of Sensitive Information it holds/processes within IFS Ultimo Information Systems to that required to deliver the Contracted Service.
6. The Third Party Supplier shall ensure that Sensitive Information shall be retained only for as long as it is required and shall be in accordance with all customer or regulatory or legislative requirements that apply.

7. The Third Party Supplier shall ensure that information is disposed of using Good Industry Practice to prevent the recovery of data. Such mechanisms include physical destruction, certified secure wiping tools and third party secure disposal services.

5. End User Access Control

1. Access to IFS Ultimo' Information Systems shall be granted to End Users in accordance with the requirements of the agreement between IFS Ultimo and the Third Party Supplier. Unauthorised access by End Users to IFS Ultimo Information Systems is strictly prohibited.
2. Records shall be maintained by the Third Party Supplier identifying the access granted to each End User. Where required, each End User shall gain access to IFS Ultimo's Information Systems using a uniquely identifiable user account which must be associated with a company email address provided by the Third Party Supplier and the use of personal email addresses (e.g. Gmail, Hotmail, iCloud, etc) is strictly prohibited.
1. End Users shall not share their account with any other End User or external third party.
2. Disclosure or dissemination of Sensitive Information by the End User regarding IFS Ultimo, its products, its customers, its partners or its Third Party Suppliers outside the official communications structures (e.g. using personal social media accounts) is strictly prohibited.
3. At no time shall an End User provide login credentials to another person unless required for troubleshooting or problem solving purposes by IFS Ultimo Corporate Services. The End User agrees to immediately notify IFS Ultimo of any unauthorised use of their account. Unauthorised individuals attempting to access IFS Ultimo or IFS Ultimo Customer Information Systems may be subject to prosecution.
4. End User passwords shall never be transmitted, displayed or printed in clear text following the initial creation of the account.
5. If passwords are shared for reasons approved by this document, then they shall be changed by the End User immediately once the need for sharing with IFS Ultimo Corporate Services has ended.
6. All End User account passwords shall adhere to the IFS Ultimo password policy complexity rules which are implemented by our Information Systems.
7. The Third Party Supplier is responsible for managing its End User Accounts and terminations and ensuring these are performed in a timely manner.
8. The Third Party Supplier shall be responsible for validating the suitability of the End User to be granted access to IFS Ultimo Information Systems. Unless otherwise agreed, such validation shall include previous employment history (3yr), right to work in country of employment and unspent criminal convictions.
9. The Third Party Supplier shall be responsible for ensuring that an account termination request is made to IFS Ultimo immediately upon change of employment status of an End User who has an IFS Ultimo managed account.
10. The Third Party Supplier shall provide, upon request from IFS Ultimo, a list of all current End Users for the purposes of supporting an audit of End User accounts managed by IFS Ultimo.

6. Handling Information Assets

1. The Third Party Supplier shall be responsible for ensuring that any End User IT assets that will connect to IFS Ultimo or IFS Ultimo Customer Information Systems have security controls installed in accordance with Good Industry Practice and, as a minimum shall include:
    a. Malware protection and be free from known viruses or malware;
    b. Patching of operating system and application software to the latest security patch level;
    c. Secure password/pin code protection;

   d. Encryption of local storage (BitLocker or equivalent);
   e. The use of approved, licenced software applications installed from a trusted source.
2. The End User shall not be permitted to remove or modify any IFS Ultimo information security software or security settings, nor use unapproved software or hardware.
3. The Third Party Supplier shall be responsible for ensuring that any IFS Ultimo or IFS Ultimo Customer information held by the End User is returned to the Third Party Supplier/IFS Ultimo or securely disposed of prior to termination of their employment with the Third Party Supplier.
4. Use of IFS Ultimo' IT assets, infrastructure, data or other facilities by the End User is provided only for fulfilment of the Contracted Service. Use in any of the following ways is strictly prohibited:
   a. Violation of local legislation or regulations;
   b. Incurring additional costs for IFS Ultimo not included within the scope of the agreement between IFS Ultimo and the Third Party Supplier;
   c. Representing a security threat to IFS Ultimo, IFS Ultimo customers or their Information Systems;
   d. For personal use including financial gain by the End User not in connection with the agreement between IFS Ultimo and the Third Party Supplier.

7. Security Monitoring & User Data Privacy

1. To the extent permitted by law, IFS Ultimo shall only monitor the activities of the End User on its Information Systems when it believes it has a legitimate business need including, but not limited to:
   a. In the course of an investigation triggered by indications of misconduct or misuse;
   b. In the course of an investigation of a suspected illegal act;
   c. As needed to protect health and safety;
   d. As needed to prevent interference with the IFS Ultimo objectives;
   e. As needed to ensure the security of the IFS Ultimo corporate network and connected services/devices;
   f. As needed to investigate an information security incident.
2. To the extent permitted by law, IFS Ultimo reserves the right to access and disclose the contents of any information held on IFS Ultimo' IT assets or infrastructure without the consent of the End User.
3. IFS Ultimo reserves the right to monitor, log and analyse all intranet and internet transmissions, site visits, internal and external service accesses, login failures, authentications, client application installs and usage, network bandwidth consumption and data transfers performed by the End User when using IFS Ultimo Information Systems and services for the purposes of:
   a. Providing IT services in accordance with their service level agreement and assuring the performance of the service;
   b. Investigating/preventing suspicious activity, potentially relating to a security breach or intruder attack;
   c. Investigating/preventing activities on IFS Ultimo IT assets, infrastructure and services which might be in breach of IFS Ultimo policies and standards.
4. Personal or sensitive information stored on IFS Ultimo' IT assets and infrastructure by the End User may be automatically backed up to secondary storage and/or accessible by authorised, privileged users. End Users shall ensure that any sensitive or personal information about themselves is only held in locations appropriate to the sensitivity of the data and ensuring that no breach of any associated data can occur.
5. Personal information disclosed by the End User to IFS Ultimo may be transferred to a company processing the personal data on our behalf (e.g. a service bureau), only in

accordance with our instructions and in accordance with appropriate confidentiality undertakings and data protection regulations..

8. Electronic Communications

1. The End User shall not create any content or otherwise transmit any information or material using IFS Ultimo Information Systems or services that IFS Ultimo believe or determines to be:
    a. Illegal;
    b. Unethical or obscene;
    c. Harassing or invades another's privacy, harms minors in any way, or promotes bigotry, racism, hatred or harm against any group;
    d. Contains derogatory or inflammatory remarks about an individual's race, religion, age, sex, disability, national origin, physical attributes, or sexual preference;
    e. Could embarrass, defame, misrepresent, or convey an unjust or unfavourable impression of IFS Ultimo or its business affairs, employees, customers, partners, suppliers, competitors or stakeholders;
    f. Infringes any third party intellectual property rights, including but not limited to copyrights;
    g. Constitutes "spam" or data virus.
2. Where IFS Ultimo provide the End User with access to the Internet and associated public facing services (including email, social media, etc.) their use is for lawful purposes only.
3. Each End User, not IFS Ultimo, shall be responsible for all content and other materials that they upload, post, email or otherwise transmit or use via the IFS Ultimo network or using an IFS Ultimo approved/supplied device across the public internet including when not in compliance with local policies, legislation, regulations or this document or in any other way in violation of expected ethics.
4. End Users shall not transmit any electronic communication using IFS Ultimo equipment or services that hides the identity of the sender nor represents the sender as someone else.
5. IFS Ultimo reserve the right to block access from within the IFS Ultimo environment and/or from IFS Ultimo equipment to any web page, internet site or service deemed unsuitable based upon the following criteria:
    a. Harmful content, e.g. containing malware or similar which might infect the client visiting the web page;
    b. Derogatory or inflammatory remarks about an individual's race, religion, political preference, age, sex, disability, national origin, physical attributes, or sexual preference;
    c. Obscene content;
    d. Content which is harassing or invades another's privacy, harms minors in any way, or promotes bigotry, racism, hatred or harm against any group;
    e. Breaks any third party intellectual property rights, including but not limited to copyrights or breaks or encourages viewers to break existing legislation.
6. The selection of which web pages, internet sites or services will be blocked shall be the responsibility of IFS Ultimo Corporate Services, Local IS, Legal, regional HR, Corporate and regional Senior Management or some combination thereof.
7. With the exception of the IFS Ultimo guest network, IFS Ultimo' wired and wireless data networks shall be used solely by IFS Ultimo owned or approved equipment.

9. Remote Working

1. All locations from which IFS Ultimo or IFS Ultimo Customer Information Systems are accessed shall provide the necessary physical security protections required to support the

processing of IFS Ultimo or IFS Ultimo Customer, information in accordance with its sensitivity. This shall include, as a minimum, any protections required by law or regulation and include protections against information being accessed, intercepted or overseen by unauthorised third parties.
2. Remote access to IFS Ultimo' data networks shall be subject to the same conditions of use as direct access to the network from within IFS Ultimo facilities.
3. External access to IFS Ultimo' data networks using non-IFS Ultimo supplied equipment shall only be permitted using approved connection methods.
4. The End User shall not connect any device to an environment that is known to be insecure, contains malware, or poses a high risk of infection to the device or IFS Ultimo network as a result of a remote connection from that location.
5. IFS Ultimo reserve the right to block access by an End User from a remote location to an IFS Ultimo network or service on the same grounds as described above from a non-remote location.
6. IFS Ultimo reserve the right to monitor the use of equipment connected to its network remotely in accordance with the same policies applicable for connection from an IFS Ultimo office location.

10. Incident Management

1. The Third Party Supplier shall be responsible for reporting to IFS Ultimo:
    a. Security incidents, including data breaches affecting IFS Ultimo or IFS Ultimo Customers;
    b. Losses of IFS Ultimo or IFS Ultimo Customer information held or processed by the Third Party Supplier;
    c. Near misses and information security concerns that could affect IFS Ultimo or IFS Ultimo Customers.
2. The End User shall be responsible for:
    a. Understanding their role in reporting and managing suspected incidents;
    b. Reporting actual or suspected information security incidents promptly and following the specified procedures applicable to their role.
3. All security incident reporting shall be in accordance with the applicable laws and regulations governing the location and nature of incident that has occurred.
4. Incidents shall be reported to IFS Ultimo via email address security@ultimo.com without undue delay and in a timescale to enable IFS Ultimo to meet its responsibilities in accordance with the applicable laws and regulations.

11. Security Education and awareness

1. The Third Party Supplier shall be expected to promote a security awareness culture through the provision of information security awareness training to its End Users.
2. IFS Ultimo reserve the right from time to time to provide security awareness training material to the Third Party Supplier for dissemination across its End User community, and where evidence of receipt and understanding by the End User may be requested.

12. Security Audit

1. IFS Ultimo reserve the right to audit the information security arrangements applied by the Third Party Supplier and, as a consequence of the findings, make recommendations for improvement or deny access to some or all IFS Ultimo Information Systems should the security controls be considered a risk to IFS Ultimo and/or its customers.
2. IFS Ultimo (or IFS Ultimo appointed independent third party auditor on its behalf and that is reasonably acceptable to the Third Party Supplier and subject to written confidentiality obligations) will examine environment and security practices relevant to the services

provided in accordance with the Third Party Supplier's agreement with IFS Ultimo in any of the following events:

a. The Third Party Supplier has not provided sufficient evidence of its compliance with the security standards set out in this document;
b. An event set out in Section 10 above has occurred;
c. IFS Ultimo or another Data Controller has reasonable grounds to suspect that the Third Party Supplier is not in compliance with the security standards set out in this document;
d. A further audit is required by IFS Ultimo' or another Data Controller's data protection authority or regulator (e.g. in case a law enforcement agency has the right to audit a Data Controller regarding the Processing of Personal Data hereunder).

3. The following audit restrictions shall apply:
   a. Unless required by applicable Data Protection Legislation, an audit is limited to once in any twelve-month period;
   b. An audit may not exceed three business days unless otherwise agreed;
   c. IFS Ultimo shall provide the Third Party Supplier with reasonable prior written notice (at least 30 days unless a data protection authority requires IFS Ultimo' earlier control under applicable Data Protection Legislation);
   d. IFS Ultimo and the Third Party Supplier shall mutually agree the scope and determine the agenda of the audit in advance. The audit shall, to the extent possible, rely on audit reports or other verifications available to confirm the Third Party Supplier's compliance with the security standards in this document and exclude any repetitive audits;
   e. IFS Ultimo shall conduct the audit under reasonable time, place and manner conditions, during regular business hours and subject to the Third Party Supplier's security policies, and may not unreasonably interfere with the Third Party Supplier's business activities;
   f. IFS Ultimo shall provide the Third Party Supplier with a copy of the audit report, unless prohibited by law. IFS Ultimo may use the audit reports only for the purposes of confirming compliance with the requirements of this document and the associated Agreement between IFS Ultimo and the Third Party Supplier;
   g. IFS Ultimo and the Third Party Supplier shall bear their own costs for the audit;
   h. If an audit determines that the Third Party Supplier has breached its obligations under this security standard or any associated Agreement, the Third Party Supplier shall promptly remedy such findings.
4. It is at the Third Party Supplier's sole discretion to determine which measures are best suitable to ensure compliance.
5. Upon IFS Ultimo's reasonable request, the Third Party Supplier will support IFS Ultimo throughout its verification processes required by the applicable Data Protection Legislation and provide IFS Ultimo with the necessary information to the extent readily available.

13. Compliance with Legislation Regarding Electronic Forums

1. Some IFS Ultimo Information Systems fall within applicable laws for responsibility for electronic forums and such regulations will at all times be adhered to by IFS Ultimo.
2. IFS Ultimo will supervise the IFS Ultimo relevant Information Systems in accordance with applicable laws and regulations and will have such control over the IFS Ultimo Information Systems as reasonably may be required.
3. IFS Ultimo reserve the right to, and will without prior notice, remove information from such relevant Information Systems, if the content of the information violates applicable laws, regulations or is deemed inappropriate by IFS Ultimo.

Review and 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, supplier confirms that it has read and familiarised itself 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.