Stork Group IT Governance:
IT compliance & security requirements

Applicable to all IT and data services delivery to Stork
This document contains the Stork IT compliance and security requirements for any vendor or supplier providing IT enabled services or handling Stork data as controller and/or processor.

Section 1: Background and scope;
Section 2: The legal terms and conditions, including audit rights and standards that are provided for in the Stork contract, supported by the Stork General Purchase Conditions. These rights and obligations are summarised in Section 2;
Section 3: The technical requirements and controls listed in this document provide the technical standards for the vendor or supplier to comply to regarding the technical and security standards of Stork and the authorised means to connect with Stork IT systems. These technical standards are listed in Section 3.

1: Background and Scope

This document outlines the minimum requirements any Stork vendor must meet to qualify for delivery of services to Stork or its affiliates or subsidiaries and applies to all IT enabled services and vendors processing, controlling, storing, transporting or accessing Stork data. An IT Governance review of all vendors deliveries will be performed to formalize qualification of the vendor and its services. This IT Governance vetting process may include questionnaires to be completed by parties. This documents intent is to provide guidance for vendors, and may be part of the agreement between parties for adherence to the compliance criteria.
For any new or renewed supplier contract, Stork must qualify the services following the Stork Group IT Governance procedure, including but not limited to a Stork Data Classification Review and reviews to assess compliance to Storks policies and standards, for which the supplier is required to cooperate fully and mandatorily deliver proof, such as documents, certificates, statements, audit reports and/or completed inquiry forms. The process will be discussed with the supplier.

2: Audit and Business Control Requirements

Third Party Independent Audit – When Storks data classification of the data exchanged between parties is designated as either "restricted' of 'confidential', a full scope audit report and/or certificate, inclusive of statements of applicability, must be provided where an independent third party auditor attests that the vendor and its sub-tiers have effective controls in place to protect customer data. This audit and/or certificate must cover all datacentres, parties having access to customer data as well as all software and application management controls. All updates and renewals must be provided to Stork without any reasonable delay without Storks request. It is not sufficient when the vendor only provides an audit report or certificate that applies to their sub-contractor or datacentre provider (Amazon, Microsoft Azure, private hosting, etc..).
The following audits standards are accepted as qualification:

Either:

- **ISAE-3402 SOC 2 Type II** (or **SSAE-18 SOC 2 Type II, SSAE-18 SOC 3 Type II, ISAE3000 SOC2 Type II) (henceforth SOC2)**

or

- **ISO/IEC 27001.**

The New Technology Assessment Procedure jointly executed by Stork and vendors will determine the data classification and if either SOC2 or ISO27001 or both needs to be the applicable standard. These accepted standard audits are applied within the generic audit rights and obligations listed in the agreement and General Purchase Conditions between Stork and vendor.
Regarding the norm **ISO/IEC 27001**, the vendor is required to hand over the valid certificate from an accredited organization, including the statement of applicability, the controls in scope and the reason why any control may not be in scope for the services provided.

Systrust or ISO Controls: The vendor shall adhere to all Systrust or ISO27001 controls/domains in their policies or practices. The certificate must reflect the vendor including its sub-tiers or sub-contractors.

Financial data: If the application contains financial data in scope for Sarbanes-Oxley a SSAE-18 SOC 1 Type II audit report or equivalent as listed above (ISAE, SSAE) must also be provided.

Data Privacy & Data Protection: Within EU countries, the applicable law & regulations of the EU country are sufficient to protect the privacy. If the vendor or its sub-tiers processes, transports, stores or accesses Stork Personal Data outside the EU region, Stork and vendor need to enter into the default EU model clauses (data transfer agreement), identifying the vendor or supplier as controller or processor. Upon suspicion of Stork data being accessed, altered or deleted by an unauthorised party, vendor must intervene, notify Stork and fully cooperate with any subsequent investigation when data was compromised.

3: IT Technical Controls

Supplier will take all reasonable measures to secure and defends its systems and data therein. Reasonable measures listed in this section, though not limited to these, are:

1) Penetration Testing: Supplier will take all reasonable measures to secure and defend its systems against hackers and those who may seek to modify or access the information transmitted or maintained by such systems without authorization.

If not already being performed as part of the Type II Audit, Supplier will perform, at its expense, penetration testing of its systems, the hosted applications, and the network perimeter for potential security breaches at least annually and will share the results of each such test with Stork or Buyer. In the event of any detected unauthorized access to and use of Stork Information or Buyer Information or passwords relating to the Supply delivered by Supplier hereunder, Supplier shall immediately notify Stork or Buyer and implement, at its sole cost and expense, Stork- or Buyer-approved remedial measures to rectify such unauthorized access. Supplier will also deliver to Stork or Buyer a root cause assessment and mitigation plan for preventing future incidents. In the event Supplier fails to remediate any security deficiency or otherwise fails to comply with the security requirements set forth herein, within thirty (30) days after becoming aware of such failure, Stork or Buyer shall have the right to conduct additional audits, testing and inspections, in addition to any other rights and remedies available to it hereunder.

2) Single-Sign On (SSO): The vendor shall allow and enable the use of SAML v2, OpenID Connect or WS-FED as the sole method of authentication for all users of the system including Stork administrators. No cloud level (native) accounts shall exist on the application to bypass SSO. Vendor support through SSO has preference, yet vendor may have non-SSO access to the application, though only via secure private connection. For applications that are used for Non-Stork access, SSO should, but may not, be available for non-Stork access: In any event it is required to enforce strong passwords with expiration and lockout. If the data is classified as Confidential and/or on Stork's request two-factor authentication must be used.

3) User data: Even if SSO is utilized, vendors should not store too much information about each user. Identity schemas should be customizable for Stork to avoid an abundance of PII – Personally Identifiable Information. For example, mobile phone or birthdate can be omitted.

4) Strong Encryption in transit: Use the latest standard encryption methods, such as TLSv1.2 for the transmission of data over ANY (public or private) networks. No custom encryption is allowed, and vendors prevent connections by depreciated protocols.

5) Mobile Device Integration: If mobile applications are available they must use the SSO system as stipulated under 2) or support strong passwords on the application as well as local encryption *derived from the password* or they must provide an option to only allow data to be downloaded onto corporate managed devices, ensuring strong encryption and authentication on the device itself.

6) Logical Segregation of Data: The application must enforce logical access control that matches the access requirements of the data stored within. Data shall only be stored within the application specific database(s) and shall not be transmitted or processed beyond the systems required to provide services

7) Documented patching practice: Documented procedures and logging for patching, security monitoring, availability monitoring, security monitoring and for backup and DR replication status. The vendor shall contractually commit to promptly (not to exceed 24 hours) remediate all security issues found in the application or system that may result in unauthorized access to data or systems. Remediation can be via a patch or configuration change in the application as long as the change does not adversely impact the operation of the application.

8) Intrusion Prevention: must be in place and actively monitored to detect and block malicious attacks. These events shall be maintained in a central system for reporting and event correlation.

9) Business Continuity/Disaster Recovery: A well-documented and tested BC/DR plan must be in place.

10) Systems Management: Remote management access to systems by administrators must be via the use of strong authentication (Including two-factor authentication) and encryption.

11) Data Transfer: An approved transfer standard, such as BizTalk, should be utilized. Files should be encrypted via PGP/GPG and the transfer should be done via SFTP. Stork should own the directory to which files are uploaded. The vendor should have a deletion process after fetching the latest file(s).

12) Firewalls: Must be configured to filter both ingress and egress traffic.

13) Network Segregation: The systems shall be hosted in a specially segmented network designed to allow access from the internet and separate from provider network. This is often called a "DMZ".

14) Audit Logs: Provider shall maintain detailed logging on all systems and applications. Logs shall contain but not be limited to recording privileged user access activities, authorized and unauthorized access attempts, and system exceptions. Software shall be present on the servers or in a central event correlation location to monitor for events that may indicate application or system compromise.