Flex Information Security Guidelines for Suppliers

1.0 INTRODUCTION

1.1. Flex aims to protect information and systems against accidental or malicious damage, destruction, modification, or disclosure. Our Suppliers play a critical role in the sustainable supply chain network and their information security posture is important for us to be able to deliver on the commitment we make to our customers.

2.0 PURPOSE

2.1. The purpose of this document is to recommend a security requirement baseline for Suppliers to protect the Confidentiality, Integrity and Availability of Flex and/or Flex Business Partners Assets.

3.0 SCOPE

3.1. This document describes at a high level of recommended security requirement to manage Information Security within the Third-Party Supply Chain network of Flex.

3.2. All the new and existing Suppliers should comply with the recommended security requirement who (i) access Flex sites, networks and/or Information Systems, or (ii) access, process, store, or transfer Flex and/or Flex Business Partner's Information.

4.0 ABBREVIATIONS

4.1. **CEO:** Chief Executive Officer
4.2. **CISO:** Chief Information Security Officer
4.3. **CPO:** Chief Procurement Officer
4.4. **MS-SDL:** Microsoft Security Development Lifecycle
4.5. **NIST:** National Institute of Standards and Technology
4.6. **SDLC:** System Development Life Cycle

flex

5.0 DEFINITIONS

5.1. **Access Control:** The processes, rules and deployment mechanisms that control access to Information Systems, resources, and physical access to premises.

5.2. **Assets:** Set of hardware, software, people, service, and Information that provides value to Flex or Flex Business Partners.

5.3. **Availability:** Information that is accessible when required by the business process now and in the future.

5.4. **Business Continuity Plan:** A plan used by an organization to respond to disruption of critical business processes.

5.5. **Business Impact:** The net effect, positive or negative, on the achievement of business objectives.

5.6. **Business Partners:** Third parties that Flex engages in commercial relationships, including but not limited to, customers, Suppliers, vendors, agents, and contractors.

5.7. **Confidentiality:** Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary Information.

5.8. **Control:** The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures which can be of an administrative, technical, management or legal nature.

5.9. **Criticality:** A measure of the impact that the failure of a system to function as required will have on Flex.

5.10. **Data Breach:** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed or a security incident that has affected the Confidentiality, Integrity or Availability of Personal Data

5.11. **Disaster Recovery Plan:** Set of humans, physical, technical, and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster.

5.12. **Encryption:** The cryptographic process of transforming data ("plaintext"), into a form that conceals the data's original meaning ("ciphertext") to prevent it from being known or used, usually by applying a mathematical function to the plaintext (encryption algorithm with a key).

5.13. **Incident:** Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.

5.14. **Incident Handling:** An action plan for dealing with intrusions, cybertheft, fire, floods, and other security related events.

5.15. **Information:** Knowledge gained through study, communication, analysis, research, etc. and/or factual data.

5.16. **Information Processing Facility:** The computer room and support areas.

5.17. **Information Security:** Ensures that only authorized users (Confidentiality) have access to accurate and complete Information (Integrity) when required (Availability)

5.18. **Information Security Risk:** Information security risk comprises the impact on Flex and/or Flex Business Partners that could occur due to the Threats and Vulnerabilities associated with the operation and use of Information Systems and the environments in which those systems operate.

5.19. **Information Systems:** An integrated set of components for collecting, storing, and processing data and providing Information and/or knowledge to manage business operations.

5.20. **Integrity:** The guarding against improper Information modification or destruction and includes ensuring Information non-repudiation and authenticity.

5.21. **Least Privilege:** The principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

5.22. **Malware:** Software designed to infiltrate, damage, or obtain Information from a computer

system without the owner's consent.

5.23. **Metrics:** A standard of measurement used in management of security related activities.

5.24. **Need-to-Know:** The principle of allowing users or processes have access only to those Information that is needed to accomplish the task and only during the time frame when it needs access.

5.25. **Penetration Testing:** A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers.

5.26. **Personal Data:** The Information or data that can be used to identify, locate, or contact an individual, alone or when combined with other personal or identifying Information.

5.27. **Policy:** Overall intention and direction as formally expressed by management.

5.28. **Procedure:** A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. It can be defined as part of processes.

5.29. **Public Domain Data:** Data or Information, regardless of form or format that an entity or person discloses, disseminates, or makes available to the public and is intended for distribution and may be freely disseminated without potential harm.

5.30. **Sensitivity:** A measure of the importance assigned to an Information, for the purpose of denoting its need for protection from any improper disclosure of such Information may have on Flex.

5.31. **Standard:** A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as ISO, NIST, etc.

5.32. **Supplier:** A person or a business firm that provides a product or service to Flex.

5.33. **Threat:** Anything (e.g., object, substance, human) that can act against an Asset in a manner that can result in harm. A potential cause of an unwanted incident.

5.34. **Virus:** A program with the ability to reproduce by modifying other programs to include a copy of itself. It may contain destructive code that can move into multiple programs, data files or devices on a system or spread through multiple systems in a network.

5.35. **Vulnerabilities:** A weakness in the design, implementation, operation, or internal controls in a process that could be exploited to violate system security.

5.36. **Vulnerability Assessment:** A process of identifying and classifying Vulnerabilities.

6.0 INFORMATION SECURITY GOVERNANCE

6.1. The Supplier should have an Information security governance framework aligned with business objectives consisting of security policies, standards, defined workflow, and metrics.

6.2. All the defined and documented Information Security Policies and Procedures should be implemented and reviewed at least on an annual basis or in other cases including, but not limited to, whenever there is a significant change in business objectives, processes, regulatory or contractual requirements. It should be approved by senior management (CEO, CISO, CPO, etc.) and communicated to all the relevant individuals including, but not limited to, employees, contractors, and temporary workers.

6.3. The Supplier should have an effective security organizational structure with significant authority and adequate resources for Information security governance.

6.4. The Supplier should ensure an independent review by a third party recognised as per industry standards, of Information Security framework (Policies, processes, Procedures, Controls, etc.) on an annual basis or whenever significant changes occur.

7.0 HUMAN RESOURCE INFORMATION SECURITY

7.1. The Supplier should perform background verification checks on relevant personnel, in accordance with applicable laws, regulations, and ethics and the verification should be proportional to the business requirements.

7.2. The Supplier should ensure that all personnel understand their responsibilities and are suitable for the roles for which they are considered.

7.3. The Supplier should ensure that all personnel has undergone appropriate Information Security training and awareness education and receive regular updates on organizational Policies and Procedures relevant to their job function.

7.4. The Supplier should have a formal and communicated disciplinary process to act against personnel who have violated any information security of Flex, based on its nature, intention, and gravity.

7.5. Upon change of job responsibilities or transfer in the role of personnel, the Supplier should make sure all the access is justified and the Need-to-Know principle is maintained.

7.6. Upon termination of personnel employment, the Supplier promptly remove access from their Information Systems, networks etc. and make sure Flex Information is protected from unauthorized access, transfer, and retention.

7.7. Other additional requirements of Information Security (if any) related to human resource must be considered as per the Flex contractual obligations.

8.0 DATA CLASSIFICATION AND HANDLING

8.1. Where Supplier's services involve accessing, storing and/or processing Flex Information, Supplier shall implement secure data handling best practices, including but not limited to Need-to-Know and limited privilege access restrictions, technical safeguards such as encryption, locked files and cabinets, and other electronic and physical security controls designed to prevent unauthorized access, misuse, loss, or theft of Flex Information.

8.2. The Supplier, when acting as a Data Processor under applicable law, should respect and apply the provisions of the Data Processing Agreement, in relation to the provided services and ensure that each of its employees and sub-processors are made aware of the contractual obligations to protect data, passing on the same contractual obligations to any subcontractors.

8.3. Among other things, the Data Processing Agreement will require that the Supplier should:

I. Only process Personal Data on the documented instructions of Flex and all applicable data protection laws, and not process data for other incompatible purposes.

II. Only outsource/subcontract with the prior written authorization of Flex and inform Flex of any changes, giving Flex the opportunity to object.

III. Assist Flex with the obligation to guarantee the rights of data subjects and fulfill Flex's obligation in this regard under all applicable data protection laws (security of Information, data protection impact assessment).

IV. Notify Flex of any legally binding request for disclosure of Personal Data processed on Flex's behalf by a law enforcement authority unless such notification is prohibited under applicable law.

V. Inform Flex about a Data Breach without undue delay.

8.4. The Supplier shall request for clarification (if needed) to Flex Business Managers on the Sensitivity and handling of Flex or Flex Business Partner's Information.

9.0 ASSET MANAGEMENT

9.1. All the Assets associated with Flex or Flex Business Partner's Information and Information processing facilities should be identified and an inventory of these Assets should be documented, maintained, and kept as a record.

9.2. Rules for the acceptable use of Information and Assets associated with Flex or Flex Business Partner's Information and Information processing facilities should be identified, documented, approved, and communicated.

9.3. All Supplier personnel shall return all the Assets in their possession that contains Flex or Flex Business Partner's Information upon termination of their employment.

9.4. Other additional requirements (if any) related to Asset management must be considered as per the Flex contractual obligations.

10.0 PASSWORD MANAGEMENT

10.1. The Supplier should implement strong password practices, including password length and complexity requirements.

10.2. The Supplier should implement a Control mechanism to verify the user identity before any password resets.

10.3. National Institute of Standards and Technology (NIST) Special Publication 800-53 can be referred for setting password Policy and its management as per the best practices.

11.0 ACCESS CONTROL

11.1. The Supplier should establish, document, and review an Access Control Policy based on business and Information Security requirements.

11.2. Unique identifications should be created for all the users and their access should be regularly reviewed.

11.3. The principle of Least Privilege and Need-to-Know should be implemented, followed, and reviewed periodically. Users shall only be provided with access to Flex or Flex Business Partner's Information for which they have been specifically authorized.

11.4. Other additional requirements of Information Security (if any) related to Access Control must be considered as per the Flex contractual obligations.

12.0 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

12.1. The Supplier should establish, document, and implement commonly accepted industry standards (MS-SDL, NIST 800-160, Secure-SDLC) to include security requirements within all phases of software development lifecycle.

12.2. The Supplier should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

12.3. The Supplier should supervise and monitor the activity of outsourced system development.

12.4. The Supplier shall take prior approval from Flex for using Flex or Flex Business Partner's Information as test data.

13.0 CRYPTOGRAPHY

13.1. The Supplier should establish, implement, and follow a Policy on the use of Encryption to protect the Confidentiality, authenticity and/or Integrity of Information.

13.2. The Supplier shall use Encryption in line with the Flex Data classification requirement for Flex or Flex Business Partner's data in transit and at rest.

13.3. The Supplier will use a reasonable Encryption Standard based on the NIST guidelines 800-175B Rev. 1. The Supplier will encrypt all Confidential Information that is:

(a) stored on portable devices or portable electronic media.

(b) maintained outside of Supplier's facilities.

(c) ransferred across any external network not solely managed by Supplier; and

(d) where required by applicable law, Personal Data at rest on Supplier's systems.

14.0 OPERATIONS SECURITY

14.1. The Supplier should develop operating procedures for the operational staff to ensure correct and secure operations of Information processing facilities.

14.2. Any changes related to business processes, Information processing facilities and systems that affect Information Security should be controlled.

14.3. The Supplier should ensure adequate security practices to detect, prevent and mitigate against introduction of malicious code like – virus, worms, malware, backdoor etc. into their Information Systems environment.

14.4. The Supplier should perform a Vulnerability Assessment and Penetration Testing on Information Systems in a timely fashion to obtain the Information related to security risks, exposures, Business Impact, etc. and based on the results, implement appropriate measures to mitigate it.

14.5. All systems and applications supporting Flex business activities directly or indirectly should be designed to log, monitor, and report security events and user activities. Logs should be tamper-proof and/or recorded on other system with minimal access on a Need-to-Know basis.

14.6. The Supplier should maintain systems that detect, and record activities like - changes, modification, processing, etc. on their Information Systems. It includes but is not limited to system logging and auditing processes, intrusion detection/prevention system, etc.

14.7. Backup copies of Information, software and system supporting Flex business processes should be taken on a regular basis in accordance with an agreed backup Policy or contractual obligations (if any).

14.8. All the Supplier personnel should participate in Information Security training and awareness sessions at least annually and Supplier should establish proof of training for all personnel. Supplier personnel may be mandated to complete Flex training and awareness program related to Information Security and Data Protection.

14.9. Other additional requirements related to operational Information Security (if any) must be considered as per the Flex contractual obligations.

15.0 INCIDENT MANAGEMENT

15.1. The Supplier should develop Incident Handling Procedures to ensure a quick, effective, and orderly response to Information Security Incidents. The Information Security events/Incidents should be reported through appropriate management channels to ensure the quick resolution.

15.2. The Supplier should define and apply Procedures for the identification, collection, acquisition, and preservation of Information which can serve as evidence or to satisfy audit requirements.

15.3. Any security Incident involving or impacting Flex must be reported to the Flex immediate point of contact. Notification should be within 48 hours from detection if Flex Data or Flex Customers' data are involved or compromised and within 24 hours for any Data Breach regarding Personally Data, as that term is defined under applicable law.

16.0 BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY

16.1. The Supplier should implement and maintain a business continuity program that includes documented recovery strategies, plans and procedures, to ensure the continuity of products and services essential to Flex within the defined timeframe.

17.0 PHYSICAL AND ENVIRONMENTAL SAFETY

17.1. The Supplier should ensure that physical security perimeters are defined and used to protect areas that contain Flex or Flex Business Partners' Information and/or Information processing facilities. Secure areas should be protected by appropriate entry/exit Controls to ensure that only authorized personnel are allowed access.

17.2. The Supplier should ensure physical protection against natural disasters, malicious terrorist attacks, epidemic, social unrest, or accidents that could lead to the loss of human lives.

17.3. All CCTV recordings and recorders must be securely located to prevent modification or deletion. Access to the recordings must be controlled and restricted to authorized individuals only.

18.0 SUPPLIER INFORMATION SECURITY MANAGEMENT

18.1. The Supplier should establish relevant Information Security requirements for their third-party vendors that access, process, store, and communicate Information of Flex and/or Flex Business Partners.

18.2. The Supplier should include requirements in the agreement with their third-party vendors to address the Information Security risks of the Information and communication technology supply chain network.

19.0 SOCIAL MEDIA HANDLING

19.1. The Supplier should not disclose any non-public or confidential data including images related to Flex and/or Flex Business Partners before receiving express written authorization in in some cases prior to signing co-marketing agreements which cover the terms and conditions of the disclosure.

20.0 COMPLIANCE MANAGEMENT

20.1. All relevant legislative statutory, regulatory, Flex contractual requirements and the Supplier approach to meet these requirements should be explicitly identified, documented, and kept up to date for the Information System and the organization.

20.2. The Supplier should ensure that their subsidiaries and subcontractors are compliant with all regulatory and local laws for the services under contract with Flex.

21.0 SUSPENSION; TERMINATION.

21.1. In addition to Flex's suspension and termination rights in any contract between Flex and the Supplier, Flex may immediately suspend Supplier's access to confidential or sensitive Information, Assets, or application if Flex reasonably determines that Supplier is not complying with the security requirements, or Supplier is reasonably determined to be out of compliance with applicable data protection or privacy laws. Flex's termination of Supplier's access shall not waive the obligation of the Supplier to perform under the agreement neither grant any rights for additional claims from the Supplier against Flex.