Supplier Information Security Requirements Policy

Integrated Management System (IMS)
Policy Owner: **Information Security Officer**
Author: **Gaurav Kumbhar**
Approval date: **08 February 2023**
Version: **V1.4**

IMAGINATION

TABLE OF CONTENTS

1. PURPOSE

The Imagination Group Limited (the "**Company"**) uses a number of suppliers who provide services and goods. The effective management of these suppliers is essential in the provision of onward services to the Company's clients and ensuring the security of the Company's systems and data. This Supplier Information Security Requirements Policy (this "**Policy**") describes control requirements for Suppliers who manage secret or confidential information.

2. SCOPE

This Policy applies to all suppliers which process, access, hold or transmit Imagination Protected Data.

3. PREFACE

Whilst it is the intention that both new and existing suppliers included in the above scope will be required to comply with this Policy, it is intended that existing suppliers will be assessed on a prioritised basis dealing with the largest and most significant first, ultimately with the aim to cover all.

All new Suppliers will be required to comply with the terms of this Policy. Suppliers of non-permanent staff (referred to as freelancers) fall under existing freelance recruitment procedures.

4. OVERVIEW

It is of vital importance to the Company that its Secret and Confidential information remains secure and protected at all times. This Policy establishes the minimum standard for information security that should be applied by relevant Suppliers to the Company on a global basis to protect the Company's resources and data.

5. DEFINITIONS

"Affiliate" means in relation to a body corporate, any subsidiary, subsidiary undertaking or holding company of such body corporate, and any subsidiary or subsidiary undertaking of any such holding company for the time being.

"Applicable Law" means (i) any and all laws, statutes, regulations, by-laws, orders, ordinances and court decrees that apply to the performance and supply of the Services and/or the handling of the Company's Protected Data; and (ii) the terms and conditions of any applicable approvals, consents, exemptions, filings, licences, authorities, permits, registrations or waivers issued or granted by, or any binding requirement, instruction, direction or order of, any applicable government department, authority or agency having jurisdiction in respect of that matter, expressly including the General Data Protection Regulation (EU) 679/2016 (the "**GDPR"**), the retained version of the GDPR in force in the United Kingdom ("**UK**") from time to time (the "**UK GDPR"**), and the Data Protection Act 2018, each as amended, modified or updated from time to time.

“Confidential Information” means information whose disclosure or loss of availability or integrity could cause harm to the reputation of the Company (or its Affiliates and/or clients), or may have a short term financial impact on the Company (or its Affiliates and/or clients).

“Information Security Incident” means (i) the loss or misuse (by any means) of any Protected Data; (ii) the inadvertent, unauthorised and/or unlawful processing, corruption, modification, sale, or rental of any of the Protected Data; or (iii) any other act or omission that compromises the security, confidentiality or integrity of any Protected Data.

“Information Systems” means all hardware, software, operating systems, database systems, software tools and network components used by or on behalf of the Company to receive, maintain, process, store, access or transmit Protected Data.

“Personal Data” means any Personal Data (as defined under Applicable Law) provided or made available to the Supplier, or collected or created for the Company (or its Affiliates and/or clients), in connection with the services that Supplier provides to the Company or otherwise in connection with the agreement existing between the Supplier and the Company. Certain types of Personal Data, such as ethnic origin or religious or philosophical beliefs, require enhanced protection and are defined as “Special Categories of Personal Data”.

“Personal Data Breach” means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any of the Company’s Personal Data.

“Protected Data” means any data or information of, or concerning, the Company or its Affiliates (or its or their clients or other recipients of the Services) that is provided to or obtained by Supplier or any member of Supplier Personnel in connection with the negotiation and execution of the agreement between the Company, or any of its Affiliates, and Supplier (the **Agreement**) or the performance of Supplier’s obligations under the Agreement, including any such data and information that either: (i) is created, generated, collected or processed by Supplier Personnel in the performance of Supplier’s obligations under the Agreement, including data processing input and output, service level measurements, asset information, reports, third party service and product agreements, and Supplier’s charges to the Company, or (ii) resides in or is accessed through the Company’s Information Systems or Supplier’s Information Systems; as well as any data and information derived from the foregoing. For the avoidance of doubt, Protected Data includes, but is not limited to, all the Company’s Secret, Confidential Information and Personal Data.

“Secret Information” means information which if incorrectly disclosed would cause exceptional or long term damage to the reputation of the Company (or its Affiliates and/or clients), or risk to those whose information is disclosed, or may have a serious or long term negative financial impact on the Company (or its Affiliates and/or clients), which, for the avoidance of doubt, shall include Personal Data or sensitive intellectual property such as embargoed products, services or information.

"Security Questionnaire” means the questionnaire designed to assess Supplier’s information security controls in alignment with industry standards (ISO 27001/27002) that is provided by the

Company and completed by Supplier.

"**Services**" means any services provided by the Supplier (including, where applicable, any Supplier Personnel or Supplier Affiliates) to Company or its Affiliates in accordance with the terms of the Agreement, including, without limitation, any deliverables, work product, materials, and documentation in connection thereto.

"Supplier Personnel" means any and all personnel engaged by or on behalf of Supplier to perform any part of the Services, including employees, freelancers and independent contractors of Supplier and Supplier's Affiliates.

6. COMPREHENSIVE INFORMATION SECURITY PROGRAMME

Supplier warrants and represents, on an on-going basis, that all answers provided by Supplier within the Security Questionnaire are accurate.

Supplier shall not materially change any aspect of the Supplier's operations that would, from the perspective of the Company, degrade or otherwise materially adversely impact the level of security provided to the Protected Data.

Supplier shall reassess against the Security Questionnaire upon the earlier of (a) any material change to any aspect of the Supplier's operations; or (b) every three years.

Where, as a result of any such reassessment, the Supplier's answers to the Security Questionnaire no longer accurately reflect the Supplier's operations, the Supplier shall promptly provide an updated Security Questionnaire to the Company.

7. REMOTE ACCESS TO IMAGINATION INFORMATION SYSTEMS

When remote access to the Company's Information Systems is required, the Supplier will be provided with secure access to an email account, an external cloud based system and/or a Company-provided laptop. Any changes to the Supplier Personnel accessing the Company's Information Systems need to be notified to the Company as soon as possible and under no circumstances shall exceed five working days.

8. PROTECTING THE COMPANY'S INFORMATION

Supplier shall implement agreed as well as general information security best practices across all supplied components and materials including software, hardware and information to safeguard the confidentiality, availability and integrity of the Company and its information. When applicable and at any time upon the written request of the Company, the Supplier shall provide the Company with full documentation in relation to the implementation of logical security and shall ensure that it has such security that:

a) prevents unauthorised access to the Company's Information Systems;
b) reduces the risk of misuse of technology service provider (TSP) systems or any Company information; and
c) detects security breaches and enables quick rectification of any problems and identification of the individuals who obtained access and determination of how they

obtained access.

9. DATA ENCRYPTION

Supplier will encrypt all Protected Data when stored on portable devices and media or when transmitted over non-secure communication channels (e.g. internet, email or wireless transmission) including remote connectivity using solutions that are certified against the U.S. Federal Information Processing Standard 140-2, Level 2, or equivalent industry standard, and will verify that the encryption keys and any keying material are not stored with any associated data.

When transferring Protected Data and in communications between the Company and Supplier, Supplier will use secure email, such as enforced Transport Layer Security (TLS), and will implement any network connectivity with the Company that Supplier is required to provide by the Company in accordance with any Company-approved connectivity standards.

In the event that Protected Data could be transferred to removable media, a mobile device or uncontrolled computer, Supplier will implement, monitor and maintain encryption and information leakage prevention tools using solutions that are certified against the U.S. Federal Information Processing Standard 140-2, Level 2, or equivalent industry standard, and will verify that the encryption keys and any keying material are not stored with any associated data.

Supplier shall prohibit the transfer of Protected Data to Supplier mobile devices where the security measures employed on such mobile devices do not meet the requirements of this Section 9 (including, without limitation, where such mobile devices do not support the technologies required to comply with such requirements).

10. ACCESS

a) General: Supplier will limit access to Protected Data to authorised persons or roles only, based upon the principle of least privilege which limits all users to the lowest permission levels that they can be assigned, but that does not prevent the relevant Supplier Personnel from completing their assigned tasks.

   Supplier must confirm the identities of all Supplier Personnel using independent, verifiable identity documents (for example, government-issued documents such as a passport or driver's licence) prior to creating any accounts for Supplier Personnel that will provide access to the Company's Information Systems or Supplier's Information Systems.

b) Passwords:

- Any passwords issued to a user by an administrator must be reset by the user upon initial use.
- Where user-initiated password resets are used, the processes that create the temporary password:
  - must create secure temporary passwords which cannot be derived from previous passwords (for example, an auto-incrementing system which generates "abc1" followed by "abc2" would not meet this requirement nor would a system which identifiably uses the current date as the basis of password generation);

- must not reuse passwords; and
- must communicate the temporary password to the user through a channel accessible only to the user.

- Where Supplier suspects any unauthorised access has occurred to any user account, Supplier shall immediately revoke the password to such user account and shall notify the Company in writing of such unauthorised access without undue delay.

11. VETTING OF SUPPLIER PERSONNEL

Supplier shall ensure that any Supplier Personnel who will have:

a) physical access to any Company site for a period of time sufficient to warrant the Company's security providing such Supplier Personnel with an identification badge permitting unescorted access; or
b) access to Imagination Protected Data,

shall have been the subject of pre-engagement screening in accordance with Attachment A to this Policy.

12. PHYSICAL SECURITY

Depending on the type of services that the Supplier is providing, one of the following (a or b) controls will be required:

a) General: Supplier shall ensure that Protected Data is physically secured against unauthorised access, including, but not limited to, by use of appropriate physical safeguards such as electronic ID card access to all areas of the Supplier's Information System.
b) Hosting: Where, and to the extent that, Supplier is providing hosting services[1] as part of the Services, it must implement the following controls as a minimum level of physical security:
   i) All hosting facilities including buildings and infrastructure shall meet the standards set out in ISO/IEC 27001 and also ISAE 3000 /3402 or such other standards agreed in writing by the Company following a security risk assessment undertaken by the Company or an independent third party.
   ii) All Protected Data processed, accessed, held or transmitted by Supplier will be physically stored in a facility subject to the following security controls:
      (1) authorised access control list requiring a photo ID check to access data centre floor;
      (2) biometric and/or keycard access to monitored man-traps leading to data centre floor;
      (3) locked server cabinets;
      (4) 24x7 indoor and outdoor CCTV monitoring with video being saved for up to 30 days or otherwise to the extent permitted under Applicable Law;
      (5) 24x7 physical intrusion monitoring alarm system;
      (6) roaming security guards; and

[1] In the context of this Policy, these physical controls for hosting services will only be applicable when Supplier hosts live services for the Company or its clients. Typically Suppliers to the Company would only host development and/or test environments on their premises. Therefore, physical access should, as a minimum, follow a).

(7) no windows are present on a data centre floor.

13. MALICIOUS CODE

Supplier will not incorporate or introduce or permit or facilitate the incorporation or introduction of Unauthorised Code into the Supplier's Information Systems nor any Company Information Systems.

Supplier shall ensure that it at all times employs adequate security practices to prevent, detect, mitigate and protect against the introduction of any such Unauthorised Code into the Supplier's Information Systems in real-time.

"Unauthorised Code" is defined as any:

a) computer virus, harmful programmes or data that destroys, erases, damages or otherwise disrupts the normal operation of the Supplier's Information Systems, or allows for unauthorised access to the Supplier's Information Systems;
b) worms, trap door, back door, timer, counter, software locks, password checking, CPU serial number checking or time dependency or other such limited routine instruction that is designed to interrupt or limit the proper operation of the Supplier's Information Systems;
c) spyware/adware; and
d) any other similar programme, data or device that is being inserted for an improper purpose.

14. NETWORK SECURITY

Supplier shall maintain and keep up to date the network component inventories, network topology diagrams, data centre diagrams and IP addresses for each network that connects to the Company's Information Systems (and their interconnections), whether supported by the Supplier, any Supplier Affiliate or a third party on Supplier's behalf, to a standard that meets compliance requirements for all connectivity to the Supplier's Information Systems from the internet, to include at least the following:

a) ensuring the network perimeter is protected by industry-leading enterprise firewall systems, including (but not limited to):
    i) establishing port, protocol and IP address restrictions that limit the inbound/outbound protocols to the minimum required; and
    ii) ensuring all inbound traffic is routed to specific and authorised destinations;
b) interrogating TCP protocol communications at the packet level to distinguish legitimate packets for different types of connections and reject packets that do not match a known connection state, i.e., stateful inspection. This must cover network, application and database protocols;
c) configuring perimeter systems with redundant connections, to ensure there are no single points of failure;
d) interrogating communications by monitoring network packets to identify and alert upon or prevent known patterns that are associated with security vulnerabilities or denial of service attacks with regularly updated signatures to generate alerts for known and new

threats;

e) maintaining and enforcing security procedures in operating the network that are at least:
   i) consistent with industry standards for such networks; and
   ii) as rigorous as those procedures which are in effect for other similar networks owned or controlled by Supplier;
f) maintaining and enforcing operational and security procedures that prevent the provision of network connectivity to third parties where such access would enable the third party to access Protected Data, or access the the Company's Information Systems should network interconnections between the Company and Supplier be enabled, without express written permission from the Company;
g) implementing perimeter management controls to ensure, at a minimum, that perimeter systems are configured to be resistant to resource exhaustion (e.g., to denial of service attacks); and
h) keeping Protected Data logically separated from all other Supplier or Supplier customer data.

15. INFORMATION SECURITY INCIDENT RESPONSE & MANAGEMENT

a) General: Supplier shall implement documented standards / procedures for dealing with any suspected and/or actual Information Security Incident against the organisation (the "**Incident Management Procedure**") and shall provide the Company with full details of such Incident Management Procedure upon request.
b) Reporting: Supplier shall, without undue delay, and,
   (i) in respect of Secret Information: no later than six (6) hours after becoming aware; and
   (ii) in respect of Confidential Information: no later than twenty-four (24) hours after becoming aware),

   notify the Company of any suspected and/or actual Information Security Incident by emailing the Company at **securityincidents@imagination.com**
c) Response & Management: In the event of an Information Security Incident, Supplier shall:
   i) take all appropriate corrective action and cooperate fully with the Company (and, where applicable, any Company Affiliates or clients) to resolve such Information Security Incident or otherwise in connection with the Information Security Incident, including identifying the Protected Data and, if applicable, persons affected, and solely at the request of the Company (and at the expense of Supplier, save where the Information Security Incident is due to the fault of the Company), providing notice to all persons whose data may have been affected by such Information Security Incident, whether or not such notice is required by Applicable Law;
   ii) where the Information Security Incident is due to the fault of Supplier, reimburse the Company (subject to the Company giving Supplier written notification of such costs together with reasonable supporting information) for all reasonable costs the Company may incur in connection with remediation efforts, including costs incurred in connection with;
      (1) the development and delivery of legal notices as required by Applicable Law and as reasonably directed by the Company where not required by Applicable Law;
      (2) the establishment of a toll-free telephone number where affected persons may

receive information relating to the Information Security Incident; and

(3) the provision of credit monitoring/repair and/or identity restoration for affected persons for one (1) year following the announcement or disclosure of the Information Security Incident or following notice to the affected persons, whichever is later, or such longer period as is required by Applicable Law;

iii) promptly, and, in any case, within five (5) days after becoming aware of the actual and/or suspected Information Security Incident, provide to the Company, in writing, a root cause analysis of such Information Security Incident. Such notice shall summarise in reasonable detail the impact of the Information Security Incident upon the Company and, if applicable, upon its Affiliates and/or clients and the persons whose data is affected;

iv) resolve and remediate any Information Security Incident within fourteen (14) days of becoming aware of the actual and/or suspected Information Security Incident as required under the documented Information Security Incident Policy. In the event that the Supplier determines that an Information Security Incident cannot be remediated within fourteen (14) days, Supplier must submit and obtain the Company's written consent to a remediation plan within seven (7) days of becoming aware of the actual and/or suspected Information Security Incident; and

v) where Supplier processes Personal Data, fully comply with its obligations under Applicable Law and under the Data Processing Agreement existing between Supplier and the Company in connection with the Information Security Incident.

16. REPORTING

At the Company's discretion and with due regard to the type of service provided, Supplier shall provide the following reports to the Company at the frequency set out below:

Report (Examples)	Description	Frequency
Service Level Agreement (SLA)	Metrics which demonstrate achievements on supplier SLAs.	Quarterly
Joiners, Movers and Leavers	Report users which need to be added or deleted from Imagination systems.	Movers and Leavers within 5 days. Joiners – per request

17. INDEMNITY

The Supplier shall indemnify, defend and hold harmless the Company and its Affiliates and the Company's or its Affiliates' Clients and the officers, employees, sub-contractors and agents of any of them against all and any actions, costs, claims, losses, damages, expenses and liabilities of whatever kind made relating to or arising out of the breach by Supplier of the terms of these Information Security Requirements.

18. AUDITING

On reasonable notice and during normal working hours, the Company shall have the right, but not the obligation, to review periodically the Supplier's and/or Supplier Affiliates' operations, processes and systems insofar as they relate to the Services for the purpose of monitoring the Supplier's and/or the Supplier's Affiliates' compliance with the terms and conditions of this Policy and/or any other additional information security requirements or practices as may be notified to the Supplier in writing from time to time. Such reviews shall not relieve the Supplier and/or Supplier's Affiliates from their responsibilities to comply with, and monitor its own compliance with, all terms and conditions of this Policy.

Supplier shall implement all recommendations resulting from any such audit having been conducted.

Attachment A
Pre-Engagement Screening

1) Screening of Supplier Personnel

a) **Screening:** Supplier shall perform the pre-engagement screening of Supplier Personnel at the time of hiring the Supplier Personnel in a manner that is consistent with the Company's minimum required screening criteria as set forth within this Attachment and as permitted by law in the country of hire.

In addition, where permitted by local law, the Company or its designated agents may perform additional screening relating to identity, criminal record and debarment of any Supplier Personnel.

b) **Cooperation:** Supplier agrees to cooperate with the Company in connection with such screening by requiring Supplier Personnel to submit information reasonably required to enable the Company or its agents to identify such personnel and conduct such screening. Should any Supplier Personnel refuse to cooperate with such screening, Supplier shall not use that person to provide the Services unless specifically approved by the Company.

Supplier shall be responsible for maintaining a pool of pre-screened personnel as reasonably necessary to support Supplier's performance of the Services.

c) **Minimum Required Screening**

i) An identity check
ii) Verification of entitlement to employment through the use of work permits or similar documents
iii) Verification of pertinent licences including motor vehicle licences, certifications and operating documents that are required by law or required due to the nature of the position/job description and/or responsibilities
iv) Previous employment reference check
v) Verification of dates of employment claimed for the previous five (5) years.

d) **Staffing Standards**: Supplier shall not permit any person to perform the Services who has been identified as having:

i) been previously employed by the Company, and whose employment was terminated with cause;
ii) false statements or claims on CV/resume/application forms;
iii) false or exaggerated educational or professional qualifications;
iv) inappropriate references from referees or previous employers;
v) relevant and/or undisclosed criminal convictions (where allowed by law);
vi) unexplained gaps in employment history;
vii) lack of cooperation; or
viii) if applicable, exclusion by the Federal government of the USA.

e) In addition to Supplier's obligations pursuant to this Section, Supplier shall use reasonable judgement, on a case-by-case basis, based on the results of such screening, when evaluating whether any Supplier Personnel should be involved in the provision of the Services given the nature of the Services to be performed by such Supplier Personnel.