Preamble

These Terms & Conditions govern the use of the Hybrid Cloud Platform – Infrastructure-as-a-Service (IaaS) (the "Service") and are to be read in conjunction with the Service Description available at the following link HCP IaaS and the relevant GMICT policies in particular, but without limitation the GMICT Information Security Policy. **IF YOU DO NOT AGREE TO THESE TERMS DO NOT USE THE SERVICE**.

Article 1.00 - Definitions

The meanings of the following words and phrases shall be as set out below:

(a) 'Client' means the persons authorised to procure IaaS Services on Hybrid Cloud Platform and / or persons authorised to administer, manage and operate resources within a Resource Group on the Hybrid Cloud Platform and shall include any Permitted Users;
(b) 'Content' includes all data input and output processed by the Solution and owned by the Client.
(c) 'Contractor' means a supplier appointed by the Client to implement the Solution and provide it with such services as may be requested by the Client.
(d) 'End Users' means the individual authorised by the Client to access the Solution and Content.
(e) 'External Resources' means such resources external to the Hybrid Cloud Platform which may need to be accessed by the Solution using adapters;
(f) 'Harden' or 'Hardening' means the removal of unnecessary software from the Resource Group to limit potential vulnerabilities that can be exploited by attackers.
(g) 'Hybrid Cloud Platform' means the On-Premises Stack (MITA Data Centre) or Off-Premises (Public Cloud) environment where the IaaS Services are provided and where Client Solutions are hosted within Resource Groups;
(h) 'Permitted User' means the individual authorised by the Client to administer, manage and operate resources within the Resource Group and includes Contractors but excludes End Users;
(i) 'Resource Group' means an environment (including virtual machines) enabling appropriate degrees of segregation and isolation, within which a Solution is hosted;
(j) 'Service' means the provision of an IaaS Service for hosting of the Solution;
(k) 'Solution means the software application or information system owned by the Client that will be accessed by the Permitted Users and hosted within the Hybrid Cloud Platform and includes the operating software necessary to operate the Solution and any database software, where applicable.

Article 2.00 - Principles

02.1 This type of hosting service enables the Client and its Permitted Users to locate the Solution in a segregated environment (the "Resource Group") within Hybrid Cloud Platform subject to the following conditions:

(a) MITA will provide the Resource Group for the Client to host the Solution and is responsible for the underlying infrastructure i.e. the Hybrid Cloud Platform;

(b) The Client will be fully responsible for operating and managing the Solution (including Content processed by the Solution) either itself or through the appointment of a Contractor. To this effect:

(i) no administration privileges will be given to MITA;

and

(ii) where the Client appoints Permitted Users, including Contractors, the Client shall obtain enforceable undertakings in terms at least as binding upon its Contractor(s) as the Client is bound to MITA in these Terms & Conditions.

02.2 The Hybrid Cloud Platform – Infrastructure-as-a-Service (IaaS) will be governed by these Terms & Conditions. In providing a Resource Group, MITA's responsibilities shall be limited to the responsibilities included in these Terms & Conditions.

02.3 The Client confirms that the Permitted Users are authorised to access the Solution in his/her capacity as employee or personnel of the Client or of a Contractor

providing services to the Client and requiring access to Solution.

02.4 The Client and the Permitted Users are required to keep abreast of the latest versions of the associated GMICT policies, standards, guidelines and directives published on the MITA website and the cloud.gov.mt portal.

Article 3.00 - Responsibilities of MITA

03.1 MITA will make available physical space within its Data Centre for the physical location of the On-Premises Stack of the Hybrid Cloud Platform. MITA will be responsible to provide:
(a) the On-Premises Stack of the Hybrid Cloud Platform;
(b) Data Centre facilities, covering electricity, air conditioning, firefighting equipment and UPS power; and
(c) Access, as may be required, to back-end infrastructure, including the Malta Government Network (MAGNET), which MITA is responsible to administer, monitor and support.
(d) Connectivity to the Off-Premises (Public Cloud) of the Hybrid Cloud Platform through MITA's Data Centre.

03.2 MITA will be responsible to manage, administer, operate and monitor the Hybrid Cloud Platform, up to the Resource Group i.e. not within the Resource Group itself.

03.3 MITA may use its own mechanisms that may be external to the Hybrid Cloud Platform in order to monitor, at its sole discretion, access to the Platform. Provided that this shall not be interpreted as an obligation on MITA to monitor and /or mange technical vulnerabilities for the Client Solution.

03.4 MITA, following discussions with the Client, will create the appropriate Resource Group and provide access to it as requested by the Client. MITA will have the final say, following appropriate discussions with the Client, to decide whether to create the Resource Group On-Premises or Off-Premises (Public Cloud).

03.5 MITA will make available tools such as, the 'marketplace' and billing portal for Clients to manage, administer, operate and monitor their Solutions within their Resource Group.

03.6 The clocks for the Hybrid Cloud Platform shall be synchronised to the Global Positioning System (GPS)

03.7 MITA will inform the Client of changes that can effectively affect Service in advance, including the following information:
(i) Categories of the change;
(ii) Planned date and time of the change;
(iii) A technical description of the change to the cloud service and underlying system;
(iv) Notification of the start and the completion of the changes.
Notifications will be sent to the email address provided by the Client.

Article 4.00 - Responsibilities of the Client

04.1 The Client will be responsible to:
(a) identify and define the necessary ICT Computing Resources that specifically addresses the requirements for the implementation of the Solution;
(b) install and configure the Solution;
(c) test the Solution; and
(d) ensure that its personnel and Contractors will maintain the necessary system security controls. MITA will not accept any liability for any harm resulting from the use of the Service.

04.2 Within a Resource Group, the Client will be responsible to fully manage the Solution, including but not limited to:
(a) all operational and administration activities, including monitoring – also from a security perspective; and
(b) the provision of maintenance and support services; and
maintaining the necessary ICT Computing Resources that specifically addresses the requirements of the Solution throughout the operational lifetime of the Solution.

User Access Authorisation

04.3 The Client is responsible to authorise access to individuals including employees and third-party subcontractors (the "Permitted Users") to perform their duties, or to execute a specific function in relation to the Resource Group. The Client shall

make such authorisation in compliance with the GMICT Information Security Policy principles.

Change Management

04.4 The Client shall be responsible for their own Change Management policy, procedure and process. The Client is strongly advised to have an appropriate Change Management framework and to follow it for all changes within their Resource Group, not only the Solution.

Patch Management

04.5 The Client shall be responsible to deploy and install any patches related to the Solution or any components within their Resource Group, in a timely manner, using their own solutions and procedures which should be built around industry recognised standards.

Maintenance and Support

04.6 The Client is responsible to ensure the maintenance and support of the Solution.

Back ups

04.7 MITA does not provide back-up services. The Client shall be responsible for any and all back-ups within the Resource Group, and all aspects related to such back-up including, but not limited to:

(a) the configuration of the backup solution / mechanism within the Resource Group;
(b) Ensuring the appropriate frequency and retention of back-ups;
(c) checking and ensuring the integrity of the data in accordance with the Client's backup procedures;
(d) diagnosing any issues with backups as they may arise;
(e) performing test restores of the backup in order to verify their integrity and restorability.

Alert Management

04.8 The Client shall be responsible to monitor and manage all alerts generated by the Resource Group including the Solution and take all the necessary and appropriate remedial action.

Software Licensing

04.9 It is the Client's responsibility to ensure that any software procured by the Client is appropriately licenced.

Quality Assurance

04.10 The Client shall be responsible to ensure that every reasonable activity has been carried out in order to attain a respectable and desired degree of quality at all times during the business analysis, design, development, testing and deployment of the Solution and any components within the Resource Group, as well as maintenance and support carried out on the Solution and any components within the Resource Group following deployment.

Acceptable Use

04.11 Neither the Client, nor its Permitted Users accessing the Service may use the Service:

- In a way prohibited by law, regulation, governmental order or decree;
- To violate the rights of others;
- To try to gain unauthorised access to or disrupt any service, device, data, account or network;
- To spam or distribute malware;

(i) In a way that could harm the Service or impair the use of the Service by another Client or Permitted User;
(ii) In any way application or situation where failure of the Service could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage; or
(iii) To assist or encourage anyone to do any of the above.

Violation of these above terms may result in termination or suspension of the Service to the extent as is reasonably necessary.

04.12 The Client shall also ensure that:

(i) The installation and use of utility programs that might be capable of overriding systems and application controls shall be restricted and tightly controlled. The Client (data owner) shall ensure that any use of the utility programs capable of bypassing normal operating or security procedures is strictly limited to authorised personnel, and that the use of such programs is reviewed and audited regularly.

(ii) Installation of unauthorised software on organisationally owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components shall be restricted. The installation of the following types of software is not allowed:

- Key loggers;
- Key generators;
- Password/Key crackers;
- Credit Card number generators;
- Network sniffing tools;
- Vulnerability / scanning tools;
- Proxy software;
- DNS software;
- E-mail client software;
- VPN client software;
- Tethering software.

Article 5.00 – Security Requirements

General

05.1 MITA implements the information security controls in accordance with the GMICT Information Security Policy and is compliant with ISO 27001 Standard. MITA is also committed to implement security controls to maintain the hybrid infrastructure compliant with best practices, including ISO 27017 and ISO 27018 applicable to the cloud environment. The controls define the administrative, physical, technical and other safeguard applied to the Hybrid Cloud Platform and describe aspects of system management applicable to the use of the Service.

05.2 The Client is responsible for any security vulnerabilities, and the consequences of such vulnerabilities, arising from the Solution or Content created, deployed or managed by the Client on the hybrid cloud.

05.3 The Client is responsible for all the security considerations within their Resource Group, including access rights granted to Permitted Users. The Client is responsible to install, configure and maintain all the security mechanisms the Client deems necessary to protect their Solution, Content and all other components within their Resource Group. The Client is urged to implement controls such as ISO 27017 and ISO 27018 or equivalent applicable to the cloud environment. For the avoidance of doubt, the Client Solution, Content or other components within the Resource Group shall not be interpreted as compliant with controls such as ISO 27017 and ISO 27018 or equivalent. MITA disclaims any liability and excludes any warranty whatsoever for the implementation of controls on the Solution, Content or other components within the Resource Group pertaining to the Client.

05.4 The Client shall be responsible for the administration, management and maintenance of end-user accounts pertaining to the Solution. This includes but is not limited to the user accounts of the operating software and of any databases, where applicable, within the Solution.

05.5 Clients creating, deploying, hosting and/or managing applications or information systems or Content on the Hybrid Cloud Platform shall ensure compliance with the Security Requirements listed in these Terms and Conditions.

End Point Security

05.6 The Client will be responsible to ensure that the Solution is protected by end-point security software compatible with its Solution. The Client will:
(a) install and configure an end-point security software;
(b) ensure regular updating of the virus definition files;

Passwords

05.7 The Client shall ensure that the Solution abides by the GMICT Password Policy available at: http://ictpolicies.gov.mt

Access Control

05.8 The Resource Group provided to the Client is Hardened. Should the Client modify such status MITA disclaims liability to the fullest extent possible.

The Client shall Harden the operating system of the Solution to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.

05.9 It shall be the responsibility of the Client to control access to program source code and associated items (such as designs, specifications, verification plans and validation plans), in order to prevent the introduction of unauthorised functionality and to avoid unintentional changes as well as to maintain confidentiality of valuable Intellectual Property.

Data Integrity

05.10 Data input and output integrity routines (i.e. reconciliation and edit checks) must be implemented by the Client for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.

Asset Management

05.11 The Client owns and controls all data input and output processed within the Solution, including Content.

05.12 Assets, including the Solution, Content and all other components stored on the Resource Group shall be removed by the Client in a timely manner upon termination or expiry of the Service, whichever the earliest.

Cryptography

05.13 The Client shall protect data in transit and data at rest through the implementation of secure versions of protocols, commensurate with the security marking of the data. Where such level of protection cannot be achieved, the Client, as Data Owner / Controller shall seek other measures commensurate with the security marking o the data.

05.14 Pursuant to the preceding Article, the protection of data may be achieved using the means that may be provided as part of the Service including but not limited to Digital Certificates and Cryptographic Keys provided that:
(a) Cryptographic Keys shall have an identifiable owner and shall be protected against disclosure, modification, loss and destruction;
(b) Digital Certificate shall abide by the terms as issued by its respective Cryptographic service provider;
(c) Both Cryptographic Keys and Digital Certificates shall be backed up and secured by the Individual responsible for the ICT device, on a location which is external to the ICT device

Data Minimisation

05.15 The Client should erase or destroy temporary files and temporary documents when no longer required.

Security Incident Management

05.16 The responsibilities of the Parties for the purpose of information security incident management shall be in accordance with the GMICT Information Security Policy.

05.17 The Client shall immediately report to the Customer any breach of security in accordance with the procedure established for the reporting of security incidents in the GMICT Information Security Policy.

Operations Security

05.18 The Client may monitor the Service through the use of activity logs, metrics and 'Application Insight' services that may be accessed via the user interface and API's available.

Business Continuity Management, including Disaster Recovery

05.19 The Client shall, where they deem appropriate, given the criticality of the Solution, implement redundancy mechanisms for business continuity purposes and perform regular checks to ensure that redundancy mechanisms are working as expected.

Information Security Tools

05.20 MITA reserves the right to carry out security assessments on the Solution. The Client shall fully collaborate with MITA in such security assessments and carry out any necessary remedial measures in order to protect MITA's infrastructure in a timely manner.

05.21 MITA reserves the right to implement the necessary security controls to detect and manage security events on the Solution in order to protect the MITA's infrastructure. The Client is expected to fully cooperate with MITA in this regard.

05.22 MITA reserves the right to install further information security tools on the Solution to enhance the protection, detection and response of such systems.

Article 6.00 - Limitation of Liability

06.1 Except as otherwise set forth in these Terms & Conditions, MITA gives no warranties, nor makes any representations, express or implied with respect to the Service and, without limiting the generality of the foregoing, all implied warranties of satisfactory quality or fitness for a particular purpose are hereby expressly excluded.

06.2 The Client will be solely responsible for the use of the Service and will indemnify and hold harmless MITA and its officers, directors, employees, agents and sub-contractors from and against any and all losses, costs, claims, damages and liabilities incurred by MITA caused by, or in any way connected with the unauthorised use of the Service by the Client or the Permitted User or any breach of these Terms & Conditions or any negligent or wrongful act of the Client or the Permitted User.

06.3 Except as otherwise provided in these Terms & Conditions, the total aggregate liability of MITA under these Terms & Conditions shall not exceed the Charges paid by the Client in respect of the Service.

06.4 MITA will not have any responsibility for ensuring the protection of third-party information. The third party shall be entirely responsible for providing the appropriate security measures to ensure protection of its private internal network and information.

Article 7.00 - Governance

07.1 MITA may carry out audits and use its best endeavours to ensure that the Client is performing its responsibilities as set out in these Terms & Conditions.

07.2 If the Client fails to take the necessary measures in the agreed timeframe, MITA shall have the right to suspend access of the Resource Group and take any additional remedial measures to totally isolate the Client's Resource Group. MITA shall consider this failure on the part of the Client as a material breach of the Terms & Conditions.

Article 8.00 – Data Protection

08.1 The use of the Hybrid Cloud Platform is governed by the Privacy Policy at https://mita.gov.mt/en/Documents/Policies/DataProtectionPolicy.pdf and incorporated within these terms and conditions by reference. MITA reserves the right to update the Privacy Policy at any time provided that such updates will not result in a material level of protection applied to Personal Data of the Client (as Data Controller) during the Term of the Service.

08.2 The Service is also governed by a separate Data Processing Services Agreement entered into between MITA and the Client. This Agreement determines the roles of the Parties for processing and controlling Personal Data. MITA will only process Personal Data residing on the Hybrid Cloud Platform as specified in these Terms and the Data Processing Services Agreement. The Client agrees to make provision for any notices required to inform the relevant Data Subjects (including Permitted Users) and obtain consent as necessary to cover the processing of Personal Data.

08.3 MITA shall not process Personal Data for the purpose of marketing and advertising.

08.4 The Client and the Permitted Users consent to the appointment of cloud service providers selected by MITA for the provision of the Service as third party processors of Personal Data for the purpose of providing the Service. The Service is contracted to the Consortium 18 Squared composed of:

- ICT Limited – Lead Member of the Consortium
- Space Hellas S.A. Telecommunications, IT, Security Systems & Services Private Enterprise for Provision of Security Services – Member of the Consortium
- Microsoft Malta Limited – Sub-contractor

MITA reserves the right to amend the list of subcontractors by providing notice to the Client and the Client may opt to terminate the agreement within thirty (30) days from the notification of such change. MITA confirms that it has entered or, as the case may be, will enter into a written agreement with the third party processor that includes substantially the same level of protection commensurate to these terms and conditions, including the Data Processing Services Agreement.

08.5 The geographical location where Client data may be stored and processed by MITA and its subcontractors is as follows:
(a) Microsoft Azure Stack: On MITA premises;
(b) Microsoft Azure Public Cloud: Primary Workloads are located in Western Europe (Amsterdam) and Secondary & DR Workloads in Northern Europe (Dublin).

08.6 The Client and /or Permitted Users may access Client Data to fulfil the Data Controller obligations to facilitate the rights of Data Subjects to access, correct and/or erase Personal Data.

08.7 For the purpose of this Article the terms "Personal Data" and "Processing" shall have the same meaning as set out in the General Data Protection Regulation (EU) 2016/679 (GDPR), and the Data Protection Act 2018 (Cap 586) on the protection of natural persons with regard to the processing of personal data, and on the free movement of such data whether held electronically or in manual form ("Data Protection Legislation").

Article 9.00 – Confidentiality

09.1 By virtue of these terms and conditions, the Parties may have access to information that is confidential to one another ("Confidential Information"). The Parties agree to disclose only information that is required for the performance of the Services under the Agreement. Confidential Information shall include the terms and pricing of this Agreement, the Client applications or information System and Client Content hosted on the hybrid cloud infrastructure and all other information identified as confidential at the time of disclosure.

09.2 The Parties agree not to disclose Confidential Information to any third party other than as set forth in these terms and conditions. Confidential information disclosed to employees, agents or subcontractors is done in accordance with these terms for the purpose of providing the Service. The confidentiality of the Client Solution and/or Content hosted on the Hybrid Cloud Platform is protected in accordance with MITA's security practices defined in these terms and conditions and the GMICT Information Security Policy. Personal Data is also treated in accordance with the Article 8 (Data Protection).

09.3 The provisions on confidentiality shall not apply in the following circumstances:
(a) the information is already known to the Party or in its possession before undertaking the obligation to keep it confidential;
(b) the information is or becomes publicly known other than through the unauthorised disclosure;
(c) the information is received from a Third Party without similar obligations of confidence and without breach of this Article;
(d) is already possessed or independently developed
(e) is required to be disclosed by order of a court of competent jurisdiction or upon the request of a competent authority; or
(f) is approved for release by written authorisation of the disclosing Party.

Article 10.00 Ownership of Rights

10.1 All Intellectual Property Rights in the Service made available to the Client and Permitted Users are the sole property of Licensor. In no circumstance shall access granted to the Hybrid Cloud Platform imply a transfer of such Intellectual Property Rights.

10.2 The Client and/or Permitted Users shall not copy, download, store, transmit, distribute, use or otherwise display any information retrieved from the Hybrid Cloud Platform. The Client and/or Permitted Users shall also not remove, obscure or change in any manner whatsoever any copyright or other notices in any material retrieved from the Service. The prohibition shall not apply to the Solution and/or Content that is owned by the Client.

10.3 The Client and/or Permitted Users may not use the Service or materials retrieved from the same in any manner that infringes Third Party Intellectual Property Rights that may be clearly defined therein.

Article 11.00 – Termination

11.1 MITA may terminate access to the Service in the case of a security violation or suspected security violation whether attributable to the Client and/or Permitted User. In the case of a security violation, the termination of access shall be with immediate effect.

11.2 The Client shall be responsible to terminate access to the Service for Permitted Users in cases where such User/s are no longer authorised and/or otherwise do not require access to the Solution and /or the Service.

11.3 Notwithstanding the preceding clauses, MITA reserves the right to suspend or discontinue the provision of the Service without notice and to pursue any remedy available at law for failure to comply with any of these terms and conditions and the relevant GMICT Policies.

Article 12.00 – Governing Law and Jurisdiction

12.1 Any dispute or claim arising out of or in connection with the use of the hybrid infrastructure provided by MITA (the "Service") shall be governed by and construed in accordance with Laws of Malta. The Parties also agree that the Courts of Malta shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with the use of the Service.

Article 13.00 – General

13.1 Any concerns and/or complaints relating to the Service, including these terms and conditions may be forwarded to cloud.mita@gov.mt.

13.2 The failure of MITA to enforce any provision hereof shall not constitute or be construed as a waiver of such provision or of the right to enforce at a later stage.

13.3 Each of the paragraphs of these terms operates separately. If any court or relevant authority decides that any of them are unlawful, the remaining paragraphs will remain in full force and effect.

13.4 We may revise these terms and conditions of use at any time by amending this page. You are expected to check these terms and conditions from time to time to take notice of any changes we made, as they are binding on you.

Last Updated: October 2020