These Terms and Conditions cover the Virtual Private Network (VPN) service which provides a secure method of network connectivity which allows permitted users to access services and/or systems hosted within the MAGNET. To this effect, these Terms and Conditions provide rules for the proper use of network and computing resources associated with this Service.

01. Definitions

01.1 For the purpose of these Terms and Conditions the following terms shall have the following meanings:

a) *'Permitted User'* means the individual accessing the System/s as approved by the Requestor;
b) *'Requestor'* means the representative of an entity providing the approval for a Permitted User(s) to use the VPN service to connect to the MAGNET;
c) *'Service'* means the provision of VPN network connectivity between the Permitted User location and the MAGNET;
d) *'System'* defines the software applications used by Government in the execution of its business and hosted by the Customer on the MAGNET.
e) *'System Owner'* is the owner of any System hosted on the MAGNET and which can therefore be accessible through this service used by Permitted User/s.
f) *'MAGNET'* (**MA**lta **G**overnment **NET**work) – the ICT and network backbone owned by the Maltese Government to provide nation-wide government services to the public sector and public service
g) *'GDPR'* (**G**eneral **D**ata **P**rotection **R**egulation) – is the data protection law of the European Union (EU) which regulates data protection amongst its member states

02. Scope

02.1 These Terms and Conditions should be read in conjunction with GMICT Policy 'Information Security Policy'

02.2 The use of the Service signifies agreement by the Requestor and the Permitted User to be bound by these Terms and Conditions.

02.3 MITA reserves the right to change, modify, add or remove any portion of these Terms and Conditions in whole or in part, at any time.

02.4 These Terms and Conditions will remain in force until terminated by either MITA or the Requestor through formal communication by email when instigated by MITA and electronic Request For Service (eRFS) if by Client.

03. Responsibilities of the Permitted User

03.1 The Permitted User understands that the credentials (username and password) required to make use of this VPN service are private and regarded as confidential information. The Permitted user therefore undertakes to maintain these credentials and any device used to store such credentials in a secure manner and also to not disclose to third parties.

03.2 A workstation with an open connection to the System must not be left unattended, particularly if the Permitted User is either directly logged onto the System or with a VPN connection to MAGNET

established. Screen savers, workstation locking, or automatic logoff shall be used to prevent unauthorised use.

03.3 The Permitted User must not choose passwords with a pattern or sequence of characters which is predictable for any other person to recognise. Passwords should never be shared and/or disclosed to anyone or used in conjunction with password-remembering applications (such as caching of passwords)

03.4 The Permitted User is given VPN access rights upon requesting the service via an eRFS. The Permitted User is then responsible for the configuration and use of the most recent software necessary to effectively use this VPN Service from his/her workstation, either by:

a) downloading the software from the URL given within the eRFS – applies for computers not joined to CORP (like personal computers); or
b) install it from the Windows Software Centre where the most recent version is made available automatically on all CORP-joined computers by MITA

03.5 The Permitted User shall:

a) not store any data owned or processed by the Government of Malta on any equipment that is used to access the System; and/or
b) not copy or extract any data owned or processed by the Government of Malta outside the System; and/or
c) In the event that, the Service is no longer being used, ensure that:
    i. any residual data which in some way appertains to the System is disposed of in a proper and orderly manner

04. Responsibilities of the Requestor

04.1 The Requestor:

a) confirms that access to MAGNET by the Permitted User is necessary in order to access Systems which are hosted on MAGNET;
b) confirms that the Permitted User is authorised to use the Service in his/her capacity as an employee or as a service provider requiring access to the System.
c) understands that access given to a System on a Corporate basis is also allowed over all VPN profiles
d) understands that access given to a System on an Organisation-specific basis is also allowed over the same Organisation VPN profile

04.2 Ensure that approvals are sought from System Owner when requesting access to Systems through this Service.

04.3 The Requestor shall immediately inform MITA by logging an eRFS if the Permitted User does not require or is no longer authorised to access the System.

05. Responsibilities of the System Owner

05.1 The System Owner is responsible for the security of his/her own system and data/information stored within it. MITA shall not be held liable for any harm to the System and/or data/information stored within, resulting from the use of the Service to use the System/s and/or of the System/s itself.

05.2 The System Owner shall assess all Requestor's requests for access to Systems before providing approvals to Requestor.

06. The Service

06.1 MITA provides access to Systems through this service as indicated in the eRFS which is considered as a form of approval from Requestor and/or System Owner to provide/configure such access.

06.2 Suspension / Termination of the Service

06.2.1 MITA reserves the right to refuse or terminate access to the Service if the Requestor or the Permitted User is in breach of these Terms and Conditions.

06.2.2 If a workstation within the control of the Permitted User is infected by malware and/or other malicious software and leads to performance degradation on the MAGNET and/or the Permitted User utilizes the Service in such a way that is detrimental to other users and/or MAGNET, MITA reserves the right to disable the Service temporarily.

06.2.3 The Requestor or the Permitted User acknowledges that in the event of security attacks originating from or using the network or components thereof of the Permitted Use as a vector, MITA will reserve the right to disconnect the Service from the MAGNET.

06.3 Liability and Disclaimer

06.3.1 Except as otherwise set forth in these Terms and 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.

06.3.2 The Permitted User will be responsible for the use of the Service and will indemnify and hold harmless MITA from and against any and all losses and damages incurred by MITA caused by, or in any way connected with the unauthorised use of the Service by the Permitted User or any breach of these Terms and Conditions or any negligent or wrongful act of the Permitted User.

06.3.3 MITA will not be held liable for any losses, or expenses of whatever nature, resulting from the unavailability of the Service at any time.

06.3.4 Neither party will be liable for any failure to perform its obligations if such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such party from transmitting or receiving any information.

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

06.4 Confidentiality

06.4.1 Each party agrees that it will not use in any way for its own account, nor disclose to any third party, any confidential information revealed to it by the other party.

06.5 Monitoring and Audit of Network Connections

06.5.1 The Permitted User acknowledges that security and operational logs of the access login to the Service will be maintained by MITA.

07. Data Protection

07.1 The Permitted User/s is required to abide by the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act (Cap 586) when accessing and/or use data stored on the Systems being accessed.

07.2 MITA shall not be held liable by Permitted User for any harm and/or damages to the Service or System caused by the misuse, be it direct or indirect, of the Service and/or System and including inappropriate use and/or disclosing Government data as regulated by the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act (Cap 586).

The General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act (Cap 586) regulate the processing of personal data whether held electronically or in manual form. MITA is set to fully comply with the Data Protection Principles as set out in such data protection legislation.

MITA collects and processes information to carry out its obligations in accordance with present legislation. All data is collected and processed in accordance with Data Protection Legislation.

The GDPR establishes a formal procedure for dealing with data subject access requests. MITA as the leading data Processor on behalf of the Government for Malta data subjects have the right to access any personal information kept about them by the MITA, either on computer or in manual files. Requests for access to personal information by data subjects are to be made in writing and sent to the DPO within their respective Ministry.

08. Modification History

Version	Date	Author	Comments
Version 1.0	23/11/2020	Reuben Camilleri	First version for release

09. Authorisation

Issuing Authority	
Signature and Date:	
Name:	Ramon Mangion
Position:	Manager

Approval Authority	
Signature and Date:	
Name:	Robert Galea
Position:	Head - ISD