Private Runtime Environment

1. Principles

A Private Runtime Environment (PRE) is an environment which enables Contractors to locate their resources in a segregated environment within premises provided by MITA. Within this environment, the following applies:

(a) MITA will provide the space for the Contractor to install its Solution;

(b) The Contractor will be fully responsible for managing its Solution;

(c) At its discretion, MITA may provide the necessary computing resources itself;

The PRE will be governed by terms of this document. The responsibilities of MITA and the Contractor in relation to the PRE are as articulated in this document.

In order to operate in a PRE, the Contractor must adhere to the following principles:

i. The Contractor fully operates and manages the Solution, including the environment irrespective whether the implementation is physical or virtual.

ii. Access from the PRE to any external resources (including databases, directory services) is governed by 'adapters'. These 'adapters' vary in shape and form, ranging from software, specialised devices / environments (such as firewalls, VLAN's), or specific operating or contractual procedures as defined in the contract between MITA and the Contractor.

iii. When the Computing Resources are to be provided by MITA, the Solution may be operational in a virtualised environment.

iv. Failure to ensure any appropriate visibility and proof that these control mechanism are in place and effective, as well as the non-adherence to any applicable policies will trigger a process where pre-established control and/or total service immobilization procedures may be considered and applied if necessary and as further defined in the Contract.

2. Definitions

i. ‘Computing Resources’ shall comprise:
(a) processing power,
(b) storage capacity, and
(c) memory.

ii. ‘Solution’ shall comprise:
(a) the application software and all its constituents,
(b) the operating software and all its constituents, and
(c) the necessary computing resources, if provided by the Contractor.

3. Roles and Responsibilities

This Section sets out the roles and responsibilities in relation to the operation and management of the PRE.

3.1 Responsibilities of MITA

In providing a PRE, MITA's responsibilities shall be limited to the responsibilities included in this section.

3.1.1 Data Centre facilities

MITA will make available the premises for the physical location of the infrastructure to be provided by the Contractor. MITA will be responsible to provide:

(a) rack space in order to rack-mount the Hardware;
(b) Data Centre facilities, covering electricity, air conditioning, fire fighting 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.

3.1.2 Provision of Computing Resources (optional)

MITA may decide to provide the necessary Computing Resources itself based on the specifications as defined by the Contractor. In such a case, MITA will also be responsible for the provision of maintenance and support on the Computing Resources.

In such an eventuality, the Computing Resources to be provided by MITA may be managed and operated by third parties appointed by MITA. MITA will co-ordinate the relationship between all parties within a spirit of commercial co-operation infusing mutual trust, commitment and collaboration to accrue increased value-added to Government.

3.1.3 Backup media administration

MITA will carry out the loading and unloading of the backup media based on a time-table to be agreed between MITA and the Contractor. As part of the backup media administration responsibilities, MITA shall be responsible for the proper storage and safe-keeping of the tapes as set out in the Operations Manual to be provided by the Contractor and agreed to by MITA.

3.1.4 Access to external resources

The specific external resources to be accessed through adapters by the Solution, if any, will be specified in the Contract entered into between MITA and the Contractor. MITA will provide access to these external resources as set out in this document.

3.1.5 Session Recording

MITA may use its own mechanisms, that will be external to the PRE in order to monitor access to the Solution by the Contractor.

3.1.6 ICT Change Management

When MITA requires to carry out a change, MITA shall notify the Contractor with the plan for the implementation of the change. It will be the responsibility of the Contractor to take any remedial action that may be necessary in order to ensure that the proposed changes have no impact on the PRE. The Contractor may request MITA to delay the implementation of the changes to allow it the time to implement the remedial action. However, MITA reserves the right to proceed with the implementation of the changes, in particular where the changes are deemed by MITA to be of a critical nature. The Contractor will be responsible to inform the entities owning the Solution of the change.

Following approval and implementation of the change, MITA shall inform the Contractor of the outcome of the change.

3.1.7 Governance

MITA may carry out audits to ensure that the Contractor is performing its responsibilities as set out in this document.

In such an event, the Contractor will ensure that its personnel, subcontractors or agents provide MITA with access to the PRE. MITA shall be bound by confidentiality where information belonging to the Contractor and/or a third party is accessed during the course of the audit.

If, as a result of an audit, MITA considers that any activity or omission by the Contractor has or could reasonably be expected to have an adverse impact on the Solution, MITA's business, activities, customers, or systems, MITA shall inform the Contractor of the actual or potential adverse impact. The Contractor shall immediately take all the necessary measures to rectify the situation within the shortest possible timeframe to be agreed upon between MITA and the Contractor.

In the event that the Contractor fails to take the necessary measures in the agreed timeframe, MITA shall have the right to suspend access of the PRE to the external resources.

3.2 Responsibilities of the Contractor

3.2.1 Implementation

The Contractor will be responsible to:

a. identify and define the necessary Computing Resources that specifically address the requirements for the implementation of the Solution;
b. procure and install the Computing Resources, if this is to be provided by the Contractor;
c. install and configure the operating software and all its constituents, and the application software and all its constituents; and
d. test the Solution.

3.2.2 Operations and Management

Within a PRE, the Contractor will be responsible to fully manage the Solution, including but not limited to:

a. all operational and administration activities, including monitoring; and

b. the provision of maintenance and support services, including on the Computing Resources (if applicable); and
c. maintaining the specifications of the Computing Resources throughout the operational lifetime of the Solution.

In performing the operations and management of the Solution, the Contractor shall abide with the following responsibilities:

(a) Access Control

The Contractor shall ensure that its personnel accessing the PRE:
(ii) are given the minimum rights and privileges needed to execute the work arrangements;
(iii) do not use the Contractor's equipment connected to the Internet, nor connect to the Internet whilst accessing the Solution, unless as provided for in this document;

The Contractor shall connect through a Virtual Private Network (VPN) in the event that the Contractor requires remote access to the Solution. If two factor authentication is required by the Contractor, the Contractor shall contact MITA in order to be provided with the code generated by the token kept by MITA.

External resources shall be accessed through the use of adapters.

Upon request by MITA, the Contractor shall provide a report listing the resources outside the PRE that are being accessed by the Solution and the tools being used for such access.

(b) Account Management

Accounts shall be assigned to individual personnel. These accounts may not be transferred to any other individual. If an individual no longer works with the Contractor, then the Contractor shall ensure that the account is immediately disabled.

Where the Contractor cannot avoid the use of specific generic accounts to operate and manage the Solution, the Contractor shall provide MITA with the procedure it shall be using for handling, storing, accessing and changing the passwords. MITA shall review the details submitted and may request the Contractor to revise such procedures to ensure an effective way of securing the passwords.

Upon request by MITA, the Contractor shall provide a report listing all accounts associated with the Contractor, their status and applicable reasons e.g. any accounts which were deleted due to the fact that employee no longer works with the Contractor.

(c) End Point Security

The Contractor will be responsible to ensure that the Solution is protected by end point security software compatible with its Solution. The Contractor will:
(i) install and configure an end point security software;
(ii) ensure regular updating of the virus definition files;
(iii) ensure regular scanning of the Solution;

(iv) update the virus signature file before each login, where possible or at lest once every week; and

(v) be capable of disinfecting the Solution and remove any viruses which are identified.

If the Contractor requires access to the Internet for the provision of this service, the Contractor shall provide MITA with the security procedures it will apply to ensure that such access does not have an adverse impact on the security of MITA's business, activities, customers, or systems.

Upon request by MITA, the Contractor shall issue a report indicating which end point security updates have been installed and which updates have not been installed and the reasons for the non-deployment. MITA may query the updates not deployed and may request that a plan of action is submitted by the Contractor for their deployment. MITA will carry regular process reviews to ensure that the end point security requirements are being adhered to.

(d) ICT Change Management

The Contractor will be responsible to have a change management process in place in order to manage changes to the Solution. The operational details of the change management process will be agreed between MITA and the Contractor and included in the Operations Manual.

When the Contractor has to carry out a change to the PRE which may impact the external resources and/or the back-end infrastructure provided by MITA, the Contractor shall notify MITA with the change and request MITA's prior approval for the implementation of the change. In such cases, the Contractor must file a Request for Change (RFC) with MITA. The RFC must include the plan for the implementation of the change. MITA will be responsible to inform the entities owning the external resources that will be impacted of the change.

MITA may (a) approve the change or (b) reject the change either by providing reasons to the Contractor for the rejection of the change or until more information is submitted by the Contractor.

Approval of the change does not mean that MITA is taking responsibility of the impact or liability that may arise as a result of its implementation.

Following approval and implementation of the change, the Contractor is responsible to inform MITA of the outcome of the change.

In those cases where the Contractor has to carry out a change to the PRE which is not envisaged to impact the external resources and/or the back-end infrastructure provided by MITA, the Contractor shall provide to MITA a list of such changes, including changes to the Solution, on a quarterly basis.

(e) Patch Management

The Contractor shall be responsible to deploy and install any patches related to:

(a) the application software and all its constituents,

(b) the operating software and all its constituents, and

(c) the Computing Resources, if applicable

using his own solutions and procedures.

The Contractor shall maintain a proper patch management procedure indicating as a minimum the method of deployment and the testing period. MITA reserves the right to review the patch management procedure used by the Contractor and may decline particular setups if these are not up to standard and recommend alternatives.

If the Contractor requires access to the Internet for the provision of this service, the Contractor shall provide MITA with the security procedures it will apply to ensure that such access does not have an adverse impact on the security of MITA's business, activities, customers, or systems.

Upon request by MITA, the Contractor shall issue a report indicating which patches have been installed and which patches have not been installed and the reasons for the non-deployment. MITA may query the patches not deployed and may request that a plan of action is submitted by the Contractor for their deployment. MITA will undertake periodic process reviews to ensure that the patch management procedure is being adhered to.

(f) Security Hardening

The Contractor is to ensure that the Solution is security hardened to ensure that those features on the ICT devices / software that are either not required for the business operation or which may pose a security risk are disabled or re-configured to minimize the associated risk.

Upon request by MITA, the Contractor shall issue a report showing the features that are disabled. MITA will undertake periodic process reviews to ensure that security hardening is being adhered to.

(g) Event Logs

The Contractor shall enable all security logs on the Solution. Such security logs, which shall be listed in the Operations Manual, shall be kept online for a minimum of 1 month.

Logs should be stored in native format. Upon request by MITA, the Contractor shall provide the security logs to MITA. MITA may also request a soft copy of the security logs, in which case the Contractor shall provide MITA with a tool which would enable MITA to read such logs without having actual access to the Solution in question.

(h) Business Continuity

The Contractor shall be responsible for the Solution's Business Continuity and shall develop any Recovery plans applicable to the Solution. The Recovery plans should cater for all instances where the Solution is affected, whether:

(a) the problem rests within the Solution; or
(b) when action is required on the Solution as a result of a problem that arises from external resources.

The Contractor shall liaise with MITA on those aspects falling under MITA's responsibilities as stated in this document and have a bearing on the Recovery plans.

The Contractor shall be responsible to provide MITA with a copy of the updated Recovery plans.

3.2.3 Maintenance and Support

The Contractor is responsible for the maintenance and support of the following:

(a) the application software and all its constituents,
(b) the operating software and all its constituents, and
(c) the Computing Resources, if applicable.

The Contractor shall immediately notify MITA of any incidents that have an adverse impact on the security of the private runtime environment together with the actions that will be taken by the Contractor in order to rectify the incident. For the purpose of incident management procedure such incidents shall be classified as critical incidents.

3.2.4 Backups

With the sole exception of MITA's responsibilities for Back-ups as detailed in Section 2.1.3 above, the Contractor shall be responsible for all aspects related to the back-ups. These responsibilities will include, but are not limited to;

(a) the provision of the back-up media;
(b) the configuration of the backup process;
(c) checking and ensuring the integrity of the data in accordance with the backup procedures
(d) diagnosing any issues with such backups as they arise;
(e) performing periodical test restores of the backup in order to ensure that written data can be read back from tape and to verify the integrity of the data.

The Contractor shall maintain proper backup procedures which will be incorporated in the Operations Manual.

MITA will undertake periodic process reviews to ensure that the backup procedure is being adhered to.

3.2.5 Alert Management

The Contractor shall be responsible to monitor and manage all alerts generated by the Solution and take all the necessary remedial action.

The Contractor may be requested to configure the Solution to ensure that all alerts are also copied to the MITA Network Management System (MNMS). The Contractor shall provide MITA with the monitoring scripts/ tools and the integration of the Solution with the MITA Network Management System based on the Simple Network Management Protocol.

The Contractor shall provide MITA with an alert reference guide which shall include an exhaustive list of events that may impact the Solution.

3.3 Summary

The table below is a summary of the Roles and Responsibilities for MITA and the Contractor for the PRE.

Function	MITA Responsibilities	Contractor Responsibilities
Facilities	1. Space for the physical location of the infrastructure 2. Data Centre facilities	1. Prepare and maintain an Operations Manual 2. Provide MITA with a copy of the Operations Manual and updates when applicable
Infrastructure	1. If applicable, provide the Computing Resources, including maintenance and support, based on Contractor's specifications 2. Access to back-end infrastructure 3. Access to external resources	1. If applicable, provide Computing Resources including maintenance and support 2. Install, configure, maintain and support the application software and all its constituents, operating software and all its constituents, and the Computing Resources
Management	1. Space for the physical location of the infrastructure 2. Data Centre facilities 3. Escalate alerts (optional) 4. Governance	1. Operate and Manage the application software and all its constituents, operating software and all its constituents, and the Computing Resources i. Establish and maintain ii. Recovery Plans for Business Continuity iii. Change Management process iv. Patch Management process
Back-up Procedure	1. Media loading and unloading 2. Storage and safe-keeping of back-up media	1. Provision of back-up media 2. Prepare and Maintain Back-up procedure as part of the Operations Manual 3. Check integrity of data 4. Periodic test restores of the backup
Alert and Incident Management	1. Configuration of MITA NMS to accept alerts (optional)	1. Prepare and maintain an alert-reference guide as part of the Operations Manual 2. Monitor alerts and take all necessary remedial action 3. Provide monitoring scripts/tools to MITA
ICT Change Management	1. Notify Contractor with changes to the back-end infrastructure and / or external resources.	1. Prepare and maintain a Change Management Procedure as part of the Operations Manual. 2. Notify MITA and seek prior approval of changes to the PRE that impact back-end infrastructure and/or resources. 3. Report to MITA changes effected to

		PRE that have not impacted back-end infrastructure and/or resources.

Adapters

4.1 Information on Adapters

The following is an example of the information to be provided about an adapter.

4.1.1. General

Service name	<<SAML Corporate Authentication Services>>
Service description	<<Authentication of Corporate Directory services through the use of federated SAML Interfaces>>
Version	<<1.0>>
Date	<<15/09/2009>>

4.1.2. Functional

(a) Consumption Information

This service provides Corporate Directory Services through the use of SAML Open Standards. These services may be accessible over http as SOAP Web Services. The Basic http/1.0 access authentication is required to access this service. The consumption of this service in secured through the use of TLS/SSL certificates for http, i.e. https.

(b) Interfaces provided

The interfaces provided for this service allow consumption to enterprise wide applications only.

(c) List of Functionality

The following is a list of functionality provided by this adapter. A detailed description of these functions is available through the adapter documentation as defined further on in this section.

- *AuthenticationQuery*
- *AttributeQuery*
- *AuthorisationDecisionQuery*

(d) Service Level

An uptime of 99% availability is guaranteed. The adapter allows 100 transactions per second and a response time of less than 2 seconds per transaction.

(e) Tools

This adapter was designed using UML tools in order to guarantee a high quality design while adopting open standards and provide for future proof and re-usability

(f) Auditing Information

This adapter, and services, monitor and log transaction details for auditing purposes. This information is limited to the usernames, service, consumer and role. An archiving process is available in line with Data Protection Policy and legislation.

(g) Standards

The following is a table with a list of standards relevant to the provision of this service.

List of Standards
SAML
http
TLS/SSL

4.2 Other terms

(a) Transactional

This service does not provide any functionality that requires transactional information.