SERVERS / SERVICES AT DATA CENTER AND CO-LOCATION POLICY

National Video Conferencing Network

Version 1.0 Released January 01, 2014

HIGHER EDUCATION COMMISSION, PAKISTAN

1 GENERAL

The Higher Education Commission has been set up by the Government of Pakistan to facilitate the development of indigenous universities to be world-class centers of education, research and development. Through facilitating this process, the HEC intends to play its part in the spearheading the building of a knowledge-based economy in Pakistan.

The Higher Education sector in Pakistan has undergone major changes in response to a rapidly – changing social, economic and political environment, and in particular, changing patterns of the deployed services and their outcome. Just as technology has transformed the way user learn, it also has the power to improve the way that institutions manage their process. The Higher Education Commission aims to give Pakistan a bright future through young, qualified and an energetic generation.

2 BACKGROUND

Interactive communication network are one of the basic ingredients and integral parts of overall building block of electronic academics (e-Academia) environment. Higher Education Commission to capitalize on the investments and efforts made to date in setting up campus-wide ICT Infrastructure and institutions and to strengthen internal as well as external communication/ network successfully initiated and rolled out a project of setting up video conference facility at each public sector higher education institution which is further led to the National Interactive Distant Learning Program (NIDLP) followed by Virtual Education Project, Pakistan.

Video Conferencing is a powerful multi-media tool that improves communication and increases an organization's productivity. It is a cost-effective way to capture these benefits without being required to travel and attend. The project aimed at bringing universities in Pakistan closer and to interact and collaborate through IP based Video Conferencing System, so that students of such universities, who are not in a position to benefit from high profiled teachers/ resources, may have the opportunity to learn from them, share their ideas and views to enhance their capabilities.

3 DEFINITIONS

Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources.

Virtual desktop infrastructure (VDI) is the practice of hosting a desktop operating system within a virtual machine (VM) running on a centralized server.

Account Information means information about you that you provide to us in connection with the creation or administration of your account. For example, Account Information includes names, usernames, phone numbers, email addresses and other information associated with your account.

API means an application program interface.

Content means software (including machine images), data, text, audio, video, or images.

End User means any individual or entity that directly or indirectly through another user: (a) accesses or uses Your Content; or (b) otherwise accesses or uses the Service Offerings under your account.

Privacy Policy means the privacy policy currently as it may be updated by us from time to time.

Service means each of the web services made available by us or our affiliates, including those services described in the Service Terms.

Service Attribute means Service usage data related to your account, such as resource identifiers, metadata tags, security and access roles, rules, usage policies, permissions, usage statistics and analytics.

Service Offerings means the Services provided by us. Service Offerings do not include Third Party Content.

Suggestions means all suggested improvements to the Service Offerings that you provide   to us.

4   PURPOSE OF DOCUMENT

This document provides a high-level scope of the Cloud architecture for Higher Education Commission. The Scope of the document covers the hosting services / servers on cloud / Data center in HEC's landscape. The objective is to offer a variety of services through the HEC Cloud to universities in Pakistan. The overriding assumption is that the cloud will be making use of the existing PERN network for broad network access to the cloud services.

5   USE OF THE SERVICE OFFERINGS

5.1 **Generally:** University / User may access and use the Service Offerings in accordance with this policy. Service Level Agreements may apply to certain Service Offerings. University / User will adhere to all rules, and regulations applicable to your use of the Service Offerings

5.2 **Third Party Content:** Such as software applications provided by third parties, may be made available directly to university by other companies or individuals under separate terms and conditions. Because we may not have tested or screened the Third Party Content, your use of any Third Party Content is at your sole risk.

6   SECURITY AND DATA PRIVACY.

6.1 Without limiting your obligations, we will implement reasonable and appropriate measures designed to help you secure Your Content

6.2 We will not access or use Your Content except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body. We will not (a) disclose Your Content to third party or (b) move Your Content by university; except in each case as necessary to comply with the law or a binding order of a governmental body. Unless it would violate the law or a binding order of a governmental body

6.3 University data will not be shared with any third party without explicit written / email permission from University's representative / point of contact, except where required by applicable law.

6.4 University's will only be managed / serviced by HEC's authorized and trained resources.

6.5 Backups can be taken and stored on a secured drive on our internal server once requested by university.

7   HEC CLOUD / DATA CENTER SYSTEM RESILIENCY POLICY

The resiliency and backups described in this Policy apply only for HEC Cloud services. University is solely responsible for developing a business continuity plan to ensure continuity of its own operations in the event of a disaster and for backing up and recovering any software.

7.1 HEC Cloud Services High Availability Strategy For business continuity in the event of an incident affecting HEC Cloud Services, HEC deploys the services on resilient computing infrastructure. HEC's production data centers have component and power redundancy with backup generators in place to help maintain availability of data center resources in the event of crisis as described below.

7.2 Redundant Power The infrastructure design includes redundant power feeds to the data center and redundant power distribution for the data center and to the data center racks. Data center cooling components (chillers, towers, pumps and computer room air conditioning units) include redundancy. The emergency standby power includes redundant battery backup with generator fuel stored onsite and contracts in place for refueling.

7.3 Redundant Network Infrastructure Network designs include redundant circuits from different carriers, firewall pairs, switch pairs, and load balancer pairs.

7.4 Redundant Program Servers University's environment consists of a set of one or more physical servers or virtual servers that provide services to University. The overall program tier functionality may be distributed across multiple physical servers or virtual servers.

7.5 Redundant Storage HEC Cloud services data resides in redundant storage configurations with protection from individual disk or array failure.

8 UNIVERSITY RESPONSIBILITIES

8.1 University is solely responsible for the development, content, operation, maintenance, and use of Content. For example, you are solely responsible for:

(a) the technical operation of Server,

(b) compliance of Your Data / Content with Policy

(c) any claims relating to Your Data / Content

(d) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Content violate such person's / company rights,

8.2 University responsible for properly configuring and using the Service and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. HEC log-in credentials and private keys generated by the Services are for your internal use only and university may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

8.3 University will ensure that all End Users comply with your obligations under this policy and If university become aware of any violation by an End User, university will immediately terminate such End User's access to Content and the Service.

8.4 University is responsible for providing University service (if any) to End Users. We do not provide any support or services to End Users.

9 PROPRIETARY RIGHTS

9.1 As between University and us, University or licensors own all right, title, and interest in and to your Content. We obtain no rights from University or licensors to your Content, including any related intellectual property rights.

9.2 Neither University nor any End User may use the Service Offerings in any manner or for any purpose other than as expressly permitted. Neither University nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any software included in the, (b) reverse engineer, disassemble, or decompile the Service or apply any other process or procedure to derive the source code of any software included in the Service.

10 OPERATIONAL SUPPORT

10.1 HEC provides assistance and consulting to the virtual machine owners. This includes recommendations for virtual machine sizing and configuration, use of tools for virtual server monitoring and performance management, and cloning and modifying existing virtual servers.

11 MONITORING AND REPORTING

11.1 HEC monitors the service infrastructure, and currently generates alerts for CPU, memory, storage, database, network components, and transactions. HEC's Operations staff attends to any automated warnings and alerts associated with deviations of the environment from HEC defined monitoring thresholds, and follows standard operating procedures to investigate and resolve underlying issues.

11.2 Due to potential adverse impact on service performance and availability, University may not use their own monitoring or testing tools (including automated user interfaces and web service calls to any HEC Cloud Service) to directly or indirectly seek to measure the availability, performance, or security of any program or feature of or service component within the services or environment. HEC reserves the right to remove or disable access to any tools that violate the foregoing restrictions without any liability to University.

11.3 University may not use nor authorize the use of data scraping tools or technologies to collect data available through the HEC Cloud Service user interface or via web service calls without the express written permission of HEC. HEC reserves the right to require University's proposed data scraping tools to be validated and tested by HEC prior to use in production and to be subsequently validated and tested annually. HEC may require that a written statement of work be executed to perform such testing and validation work.

11.4 HEC will provide University with access to a University notifications portal. This portal will provide metrics on the System Availability Level for Cloud Services acquired. For those Cloud Services for which such metrics are not available via the University notifications portal, HEC will provide metrics on the System Availability Level upon receipt of a Service Request submitted by University to HEC requesting the metrics.

12 HEC CLOUD / DATA CENTERS CHANGE MANAGEMENT POLICY

12.1 HEC Cloud Operations performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software to maintain operational stability, availability, security, performance, and currency of the HEC Cloud. HEC follows formal change management procedures to provide the necessary review, testing, and approval of changes prior to application in the HEC Cloud production environment.

13 EMERGENCY MAINTENANCE

13.1 HEC may periodically be required to execute emergency maintenance in order to protect the security, performance, availability, or stability of the production environment. Emergency maintenance may include program patching and/or core system maintenance as required. HEC works to minimize the use of emergency maintenance and will work to provide 24 hours prior notice as of any emergency maintenance requiring a service interruption.

14 MAJOR MAINTENANCE CHANGES

14.1 To help ensure continuous stability, availability, security and performance of the Cloud Services, HEC reserves the right to perform major changes to its hardware infrastructure, operating software, applications software and supporting application software under its control, no more than twice per calendar year. Each such change event is considered scheduled maintenance and may cause the Cloud Services to be unavailable for up to 24 hours. Each such change event is targeted to occur at the same time as the scheduled maintenance period. HEC will work to provide up to 60 days prior notice of the anticipated unavailability.