





DOCUMENT CONTROL BLOCK				
	Document Code: Applications and Digital Channels Compliance Requirements	Version: 1.0	Issued On: 27/01/2021	 وزارة الموارد البشرية والتنمية الاجتماعية المملكة العربية السعودية
	Title: Applications and Digital Channels Compliance Requirements for Vendor's Management		Page 1 of 7	

Applications and Digital Channels Compliance Requirements For “Bidders’s Management”

DOCUMENT CONTROL BLOCK				
	Document Code: Applications and Digital Channels Compliance Requirements	Version: 1.0	Issued On: 27/01/2021	 وزارة الموارد البشرية والتنمية الاجتماعية المملكة العربية السعودية
	Title: Applications and Digital Channels Compliance Requirements for Vendor's Management		Page 2 of 7	



Date: 10-Nov-21

Revision History

Date	Author	Version	Description of Addition/Update
18 Jan 2021	Abdullah Alsamsam Shareef Saqer	2.3	Update, add
27 Jan 2021	Ahmad Alahmad		



Approval

Name	Position	Signature
Unit Head Name		

DOCUMENT CONTROL BLOCK				
	Document Code: Applications and Digital Channels Compliance Requirements	Version: 1.0	Issued On: 27/01/2021	 وزارة الموارد البشرية والتنمية الاجتماعية المملكة العربية السعودية
	Title: Applications and Digital Channels Compliance Requirements for Vendor's Management		Page 3 of 7	

Introduction and Guidance:

1. The Bidders should confirm full understanding, consideration, compliance, and readiness for Applications and Digital Channels Compliance Requirements listed in this document.
2. The Bidders must respond to each point, and provide applicable details and best practice for the following:
 - Compliance level (Fully Compliant, Partial Compliant, or Non-Compliant).
 - Description and clarification for how the requirements will be covered, and/or understanding of it, based on MHRSD's Applications and Digital Channels Compliance Requirements Check List for document, and Reference from provided Proposal, for all points mentioned in Document.
 - For any Partial Compliant or Non-Compliant, Bidders should provide detailed explanation for the alternatives or the work around solutions for the required controls.

DOCUMENT CONTROL BLOCK				
	Document Code: Applications and Digital Channels Compliance Requirements	Version: 1.0	Issued On: 27/01/2021	 وزارة الموارد البشرية والتنمية الاجتماعية المملكة العربية السعودية
	Title: Applications and Digital Channels Compliance Requirements for Vendor's Management		Page 4 of 7	

Applications and Digital Channels Compliance Requirements

Version: **1.0** Updated On: **Jan 27 2021**



In order to ensure provided Products / Solution meet minimum criteria during evaluation, this set of Applications and Digital Channels Compliance Requirements should to be verified during the procurement and proposals submission process.

Compliance should be in C1 (Full Compliance), C2 (Partial Compliance with justification), C3 (Non-Compliance).



Bidders Name: XXXXXX

Contract-ID: XXXXXX



#	MHRSD's Applications and Digital Channels Compliance Requirements	Compliance			Comments
		C1	C2	C3	
Source Safe	Saving all code in source safe (e.g. TFS)				
	Code is owned by HRSD				
	Before closing the project, uploading latest source code to source safe				
	Code versioning and branches based on features and customizations				
	All Documents (Technical – Business – user guides) also saved to source control with versioning				
Coding Standards	Providing source code standards to be approved by HRSD				
	Code must be well structured, readable, Maintainable and well commented.				
	Code will be review by HRSD based on approved standard.				
	Multiple tier architecture code				
	Separating between layout code and other layers (models, logic, data...) with providing complete design and UI toolkit.				
	Avoid repetitive codes by building and using reusable components or libraries in different layers with documentation and guide for reuse.				

DOCUMENT CONTROL BLOCK				
	Document Code: Applications and Digital Channels Compliance Requirements	Version: 1.0	Issued On: 27/01/2021	 وزارة الموارد البشرية والتنمية الاجتماعية المملكة العربية السعودية
	Title: Applications and Digital Channels Compliance Requirements for Vendor's Management		Page 5 of 7	

	Applying powerful logging mechanism that support troubleshooting issues				
	Portable code works on multiple environments				
	Exception and error handling should be clear and descriptive				
	Following secure coding standards to prevent security vulnerabilities referenced to OWASP and NCA				
Mobile Standards	Latest guidelines from Apple and Google				
	Using native mobile application development				
	Support Latest update from Apple and Google				
	Data Encryption				
	Support for New Devices during the development and support lifecycle				
Technology Standards	For open source technology use YESSER open source rules and open source rules (OSS standard 1.0) reference				
	Support integration with NIC IAM for all platforms (i.e. Authenticate users)				
	Internal applications using Active Directory (i.e. Authenticate users)				
	Support customization and flexibility on different platform components (authentication, authorization, integration ...)	-			
	Well known and high reputation languages and technologies	-			
Integrations Standards	Using API/Services instead of database-to-database integration.			-	
	Using the integration layer (ESB layer in HRSD).				
	Using iPaaS for integration.				
	Using REST-full APIs.			-	
	Following Open APIs standards.			-	
	Using secure communication TLS v1.2 or higher.			-	
	Encrypting sensitive data.	-			
	Support API/Services versioning.			-	

DOCUMENT CONTROL BLOCK				
	Document Code: Applications and Digital Channels Compliance Requirements	Version: 1.0	Issued On: 27/01/2021	 وزارة الموارد البشرية والتنمية الاجتماعية المملكة العربية السعودية
	Title: Applications and Digital Channels Compliance Requirements for Vendor's Management		Page 6 of 7	

Service life cycle (from establishing the service, until termination).			-	
All API/Services should be Stateless.			-	
Using API Keys or client certificates for system authorization instead of using username/password.			-	
All API/Services should have a defined SLA.			-	
All API/Services Subscription should have SLA.			-	
Quasi Static data should be cached by invoking system (consumers).	-			
Using DNS names instead of IPs for communication.	-			
All API/Services should be modular and self-contained			-	
All API/Services should have proper documentations (swagger file, fields description ...etc.)			-	
Online point to point integration might be allowed in very special cases after getting design authority exceptional approval.			-	
Integration should not hold any business data, rules or logic unless approved. As those should be hosted in related business application/modules			-	
Integration API/Services can be aggregation or orchestration of multiple related APIs, providing new business capabilities.			-	
Retry and rollback behavior should be well documented in any management/transaction/writing interface.			-	
Maintaining proper log/audit/dump level while maintaining privacy of sensitive and secure data.	-			
API which will be exposed to integration: should has access to all the data it needs locally. <small>Future-roadmap</small>			-	
No critical dependencies between API/Services, i.e. availability, development deployment of a service should not interfere with other services. <small>Future-roadmap</small>			-	

DOCUMENT CONTROL BLOCK				
	Document Code: Applications and Digital Channels Compliance Requirements	Version: 1.0	Issued On: 27/01/2021	 وزارة الموارد البشرية والتنمية الاجتماعية المملكة العربية السعودية
	Title: Applications and Digital Channels Compliance Requirements for Vendor's Management		Page 7 of 7	

Releases Standards	Delivering release note			-	
	Release management from Governance document			-	
	Providing release script and mask the sensitive data (for non-production environments)			-	
	Using auto deployment on all environments with best practice polices of manage and approvals			-	
Required Environments	Having five environments development, testing, pre-production, production, and disaster recovery environments		-		
	High available production environment and disaster recovery environments for applications and databases	-			
	Full separation between environments especially between production and none-production environments		-		
Technical Deliverables Standards	Delivering All Documents (Business – technical – Testing – user guide)			-	
	Delivering source code	-			
	Approving source code by HRSD			-	
	Minimum required Technical Documents: <ol style="list-style-type: none"> 1. Business Requirements Document BRD 2. Software Requirements Specification 3. Design Document (HLD and LLD) 4. Integration Requirements 5. Prototype and Demo Sessions 6. Design Guide Line (HTML template – assets) including : <ul style="list-style-type: none"> -Style - Layout - User interface (UI) components – e.g., menus, buttons -Text – e.g., font, tone, labels/fields - Accessibility – e.g., Aria markup for disabled users -Design Patterns – e.g., forms 		-		