ANNEXURE E – FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

1. Video Wall Requirements

Requirement ID	Requirement	Requirement Description
VS_01	Uninterrupted content display	The video wall displays must be set up such that content is displayed over them continuously.
VS_02	Content Management Software	The solution must incorporate Content Management Software that will configure and control the content displayed.
VS_03	Easy installation and maintenance	Video walls must be made up of thin, lightweight displays that can be easily moved and reassembled and maintained.
VS_04	Content Scheduling	The solution must make provision for prescheduling of content, that can be played at any time.
VS_05	Digital Media	The desired video wall solution must support digital media formats such as images, videos, and graphics.
VS_06	Remote Management	Authorised users must be able to manage and monitor the display network remotely.

VS_07	Data Encryption/Decryption	The video wall display must not hold any memory, and its secure operating software should be capable of encrypting and decrypting data.
VS_08	High image quality	The video walls must be made up of multiple displays that work congruently to act as a single display, so image size can be scaled up—or down—without sacrificing image quality.
VS_09	Video Wall Processors	Processor/controller must be able to take inputs from various sources and put them all together, for display on multiple screens.
VS_10	Dedicated PC for Setup and Control	The videowall controller must be connected to a dedicated PC that will not only serve as a user interface, but also initiate control commands to the processor. Using an external PC isolates control functions from on-board processing resources. This eliminates operational load on the CPU, optimizing response time and speed when recalling window pre-sets or performing other operations, especially with large systems.
VS_11	Remote System Control	A simplified control interface with a series of button selections, so a user only needs to control the most

		common or essential functions on a videowall – selecting an input source or a pre-programmed window pre-set.
VS_12	Large Facility Control	Management of all communications, including AV, must be centrally integrated into a single control system to allow multiple room operations to be performed from a common GUI.
VS_13	On-Demand Control	The system must be equipped with a limited number of pre-defined window layouts, plus the ability to change source window inputs to provide the flexibility for authorised users to change the window layouts as when required.
VS_14	Integrated view of operational information	The solution must provide an integrated view of critical operational information, to enable collaboration within the value chain.
		The solution must deliver seamless integration of both near real-time and historic information
VS_16	Multi-level security access protocol	Intrusion prevention to the SP facilities where media is stored is required in the form of a multi-level access protocol e.g. • Level 1: Key-card and pin-pad combination to get access to the building • Level 2: Biometric scan (e.g., fingerprints) to authorize entry • Level 3: Secured cabinets requiring a PIN that only authorized personnel know

VS_17	Plug-and-play installation	The video walls must have capability to be relocated and reinstalled when the need arises.

2. Digital Signage Requirements

DS_REQ01	Content Management System	Content Creation — Create content and update the CMS with new content Hardware Management — capability to assist system administrators monitor and manage digital hardware, including players and screens. Content Download
DS_REQ02	Content Publication	Transmit dynamic and static content for display at multiple sites. Capability is required for different content to be displayed on different channels at different times.
		Single Screen/ Single Zone display Single Screen/ Multi Zones display Multiple Screens/ Multiple Zones display with same content on all the screens Multiple Screens/ Multiple Zones display with different content in different screens
DS_REQ03	Emergency Content Push	The Digital Signage solution must have capability to "Push" Emergency Content and interrupt any previously displayed Content at individual sites at different times.

		Emergency content pushing must be centrally controlled, with restricted access.
DS_REQ04	Dynamic Content Update	System must automatically refresh itself when new Content is received. It must be possible for the screens to flip between displayed Content
DS_REQ05	Near-Real Time KPI reporting	The required solution must be capable of integrating with TFR's existing reporting system to extract reports in Real-Time.
DS_REQ06	System uptime monitoring and warnings of downtime	When system downtime or faults occur, an automatic escalation/alert must be sent to a TFR Service technician to investigate.
		Issues/faults unresolvable by TFR's service technicians must be escalated to the Service Provide for action.
DS_REQ07	Report Generation	The DS solution must enable generation of reports that show periods and durations of screen downtime.
		It must be possible to draw reports from the system of archived content.
		System up-/down- time logs
DS_REQ08	Ticker Tape	The solution must provide scrolling text display capability at the bottom of the screen. Messages can be time-sliced to ensure that the correct messages are scrolling across the screens at the appropriate time of day.

DS_REQ09	Flexible playlists	The system must have capability to create playlists, smart playlists and sub-playlists
DS_REQ10	Schedules	Capability is required to define and edit playlist time slots with variable recurrence patterns and start/end dates.
DS_REQ11	Multi-channel Support	The system must be able to run two entirely separate channels from a single player
DS_REQ12	Workgroups/Area	Capability to manage access to content for different locations so that it can be possible to show content in specific areas that is only relevant to them E.g., a weather warning in a particular region
DS_REQ13	Approvals	Approve content before media can be played. Selected users will be notified by email when an approval is required.
DS_REQ14	Player Management	Capability required to group Players by criteria (geography, demographics, etc.) set playback options and select content to play.
DS_REQ15	Maintenance Scheduling	Conduct remote maintenance tasks such as reboot, send and retrieve files or install software updates.
DS_REQ16	Live Data Feeds	The system must have capability to integrate live data sources directly into the digital signage content.

3. Non-Functional Requirements

Requirement ID	Requirement Description	Requirement Detail	
NFR_01	Performance	High quality playback	
NFR_02	Capability & Scalability	The required software should be scalable, in order to accommodate potential growth of the digital network.	
NFR_03	Reliability	High uptime and stability	
NFR_04	Storage	• Capability required to save media files on the internal storage, ensuring uninterrupted playback in case of loss of internet connectivity. • The digital signage software should offer unlimited file storage	
NFR_05	Availability	• The DS screens must be available 24/7 and must never be blank. • Remote Monitoring and Network Dashboard – The preferred digital signage software should include a dashboard that allows for status monitoring of the digital signage network.	
NFR_07	Operability	The DS system must be easy and convenient to learn and operate.	
NFR_08	Security – Physical	• Wiring closets to secure media players behind lock and key • Enclosures or other physical lock-down devices for media players connected at display in public areas • Enclosures or mounting systems to protect and secure display screens • Placement of display to deter smash-and-grab tactics	
NFR_09	Security – Device Level	Local Accessibility	• Physical installation should be safe from radio interference, and any CD/ DVD drive access, power buttons and remote control (infrared) ports should be locked, secured and generally inaccessible. • Available ports should require authentication for use, and no automatic run settings should be activated when peripheral devices (e.g., keyboard or mouse) are connected. Therefore, it should not be possible to simply push content into the player by inserting a CD/DVD or USB card.

		BIOS or Boot-ROM	• The BIOS controls features such as the boot order, which determines the sequence hard drives and other storage devices are considered for locating and launching the operating system. To ensure security during this process, only the secured storage devices should be configured in the sequence.
		Operating System	• The operating system (OS) must restrict or remove the launching of nonessential services by evoking only the services required for the operation of digital signage media player devices. The removal of these additional services offers security benefits such as: o Lower memory utilization o Smaller attack footprint (lower chance a vulnerability will be present in the software components) o Ease of maintenance o Fewer moving parts leading to fewer conflicts and bugs • On the media players, no paths must exist to load third (3rd) party applications, spyware, or viruses, i.e., media players must be dedicated and optimized for the sole purpose of playing digital media.
		Network Security	• Media players should only speak to their host servers, or other authorized servers (e.g., Content Distribution Network or CDN, RSS sources) • Media players should have a software firewall enabled as an extra layer of "just in case" security • Media players should be installed behind a NAT device to create a firewall between the media player device and the Internet. This makes it far more difficult for a remote attacker to gain access to the media player device

			• Media players should use standard protocols like FTP and HTTP for data transfer.
			• Media players should only support encrypted wireless networks which require authentication to access
			• Media player control protocol should be simple, transparent and based on standards.
			• The Digital Signage should also support:
			  ○ VPNs – Virtual Private Networks – to facilitate encryption of all traffic.
			  ○ HTTPS - A standard and highly secure mode for bi-directional encryption of information.
			  ○ Authentication and Identification – Protocols that allow for secure identification should be used when available. If not, the vendor's protocol should allow for some level of identification to ensure that the player is receiving trusted information from the servers it communicates with.
			  ○ Media players should be behind a NAT (Network Address Translation) firewall that only allows outbound connections to be established

		Software Security	• Antispyware and virus protection systems must be in place at local level. • The user software should have a robust personalization engine to create and enforce role-based security and authentication. Each user that is created in the system should be able to create a unique password that is tested for strength during the creation process. This ensures appropriate security

			measures are taken at the user level.
		Operations Security	• The system must enforce regular changing of passwords. • Implementation of normal IT precautions such as patching servers with software updates for security issues • Servers must be monitored, and intrusion detection systems must be in place. • Security audits must be run routinely so that possible breaches can be timeously detected and eliminated. • Capability must be in place to have media players report on their health
NFR_10	Interoperability		The DS system must be capable of integrating with TFR backend systems, for real-time information that could possibly be displayed on the screens, e.g., train deviations, incident notifications, etc.
NFR_11	Recoverability		System should not take too long to get up once it has been down (not be down for over 3hrs) and information must be recoverable up to a point where the information was last saved.
NFR_12	Role-Based Access Control		User's system privileges will determine the type of access that they have to maintain and upload content to the visual devices.
NFR_13	Content Ownership		Ownership of all content must remain with TFR