TrackerHero Sdn. Bhd.

REAL TIME MONITORING SPECIFICATION

No	Specification	Category	Yes/No	Reference
A	Software & Hardware			
1	Real Time Patrolling System – www application	Software	Yes	
2	Real time – On the spot data transfer		Yes	
3	Real-Time Clocking with Visual Report		Yes	
4	Trail tracking (route of the device)		Yes	
5	Processing alarm event		Yes	
6	Visitor Management System		Yes	
7	Face Recognition Attendance System		Yes	
8	Situational Report (SITREP)		Yes	
9	Incident Report		Yes	
10	Local cloud server		Yes	
11	Voice communication – Two – way voice communication device		Yes	
12	Panic Button	Hardware	Yes	
13	GPS tracking		Yes	
14	Geofencing (boundary of pre-determined zone)		Yes	
15	IP 67		Yes	
16	Shock detection – device drop detection		Yes	
17	Man down detection		Yes	
18	Sabotage detection		Yes	

No	Specification	Category	Yes/No	Reference
19	GSM/GPRS	Hardware	Yes	
20	Local cloud server		Yes	
21	RFID/NFC reader – for checkpoints		Yes	
22	Handy, waterproof and shock resistant casing (rugged)		Yes	
B	Cyber Security			
1	Any ICT infrastructure and web applications to be assessed for vulnerabilities and remediated prior to production deployment	General Security Requirement	Yes	
2	Connections to the public cloud must be private	Telecommunication Networks	Yes	

3	Authorized SIM card per device
	• to use a private Access Point Network (APN) which can limit the access from/to internet
	• to secure the SIM card:
	  • IMEI/MSI matching
	  • APN password
			Yes	

4	The data center shall comply with the regulatory or industry compliance: • ISO 27001 - Information Security Management System • Personal Data Protection Act (PDPA)	Data Center/Cloud	Yes	
5	Disaster Recovery Plan established to ensure business continuity		Yes	
6	Servers should be installed with antivirus to prevent any malware or virus infecting to the machine		Yes	
7	Controls against Distributed Denial of Service attack • All data center providers shall have protection against DDOS attack		Yes	

No	Specification	Category	Yes/No	Reference
8	The system shall use encryption to ensure sensitive data is transmitted over secure platform (eg certificates, keys)	System and Applications	Yes	
9	The system is able to use secure communication as below: 1. At least TLS version 1.2 or higher 2. Secure TLS cipher suites TLS_ECDHE_ECDSA_WITH_AES_256		Yes	
10	The solution shall comply with TNB password policy: Force users to change passwords after 90 days. • Minimum password length at least 8 characters • Consists of numbers, uppercase/lowercase letters, special characters • Prevent re use of recently used passwords; at least the last 4 passwords		Yes	
11	Account lock out shall be in-placed after pre-defined number of consecutive failed authentication attempts by the user		Yes	
12	Account timed-out should be in-placed. Idle or inactive sessions for more than the pre-defined time will require re authentication		Yes	
13	All user accounts are assigned to appropriate user groups or application roles to ensure proper authorization and assignment of privileges to users		Yes	
14	Audit trail of all critical events including, but not limited to, are enabled :- a. All successful and unsuccessful login attempts b. All administration activities c. All access to sensitive/confidential files and details of access.		Yes	
15	Voice Calls from/to the PATROL DEVICE must be filtered to prevent misuse of the device	Patrol Device	Yes	

No	Specification	Category	Yes/No	Reference
16	Remote configuration should be secure (either via SMS or Web Services) • If remote configuration via SMS has to be allowed, it should be allowed from the registered number only. Else disable the SMS service • If remote configuration via web services has to be allowed, it should allow from a Mobile Device Management (MDM) solution and authentication shall be made mandatory	Patrol Device	Yes	
17	Any tampering events (e.g. Opening the PATROL DEVICE's back cover) should be logged and sent to the system		Yes	
18	No usage of third party applications which may leak sensitive information to third party • The function of Patrol Device should be limited to only patrol activities. • Usage of third party application in the Patrol Device should be avoided or kept at minimum.		Yes	
19	Authentication is required for local device configuration • Any installed software that has privilege to do local configuration shall support an authentication before usage OR • To enable device authentication before any configuration or connections made to the device.		Yes	
20	Device Storage - Storage Encryption If the device contains sensitive information, the device storage shall be non-readable or can be remotely deleted, should the device be misplaced or stolen.		Yes	
21	The vendor should ensure that all confidential/sensitive information is exchanged via a secure protocol (e.g. HTTPS) from the PATROL DEVICE to the backend system (server/cloud).		Yes	