TERMS OF REFERENCE FOR SUPPLY, DELIVERY, COMMISSIONING AND MAINTENANCE OF UNMANNED AERIAL VEHICLE (UAV) - DRONES

1. Executive Summary

The proposed tender seeks to procure for the supply, delivery, commissioning and maintenance of Unmanned Aerial Vehicles (Drones) aimed at modernizing Kenya's enforcement and border management operations. The deployment of the 4 drones and a fully integrated command and control center will result in enhanced security, improved revenue assurance, and strengthened border control activities across the country. Leveraging on the drone technology will give the authority real-time videos of various operational areas and centralized monitoring will improve accountability. The drones will address existing operational challenges in encountered in hard and unsafe areas to patrol physically while ensuring seamless integration with current and future Customs systems. The selected vendor will be responsible for supply, delivery, and commissioning, training over an 18-month implementation period and 1-year warranty period and long-term support will also be provided ensuring sustainable, secure and efficient operations nationwide.

2. Background

The Kenya Revenue Authority (KRA) is tasked with collecting revenue for the Government of Kenya, with the Customs & Border Control Department playing a crucial role in facilitating international trade and enforcing border security. This mandate includes expediting the clearance of goods, regulating imports and exports, collecting revenue, and enforcing legal prohibitions and restrictions to protect society and the environment. The current rapid advancement of technology in recent years has necessitated significant improvements in the way Customs operate. To meet the growing demands for enhanced border security, efficiency and revenue mobilisation the acquisition of Drones has become increasingly critical for KRA.

3. Objectives

- **Enhanced Border Security**: Ability to perform patrol and surveillance activities remotely and 24hrs a day help deter criminal activities.
- **Efficiency in Border Management**: Facilitate the efficient management of our borders through reduction in illegal entry points.
- **Remote Monitoring and Control**: Enable remote monitoring and control of border patrol operations, enhancing convenience and security.
- **Integration with Surveillance Systems**: Integrate with video surveillance to provide real-time monitoring and alerts for suspicious activities.
- **Enhanced Revenue Collection** – Reduced smuggling activities and compliance will lead to enhanced revenues.
- **Reduced Operating Costs** – Automation of patrols will be efficient and will lead to lower operating costs.

4. Scope of work

The scope of the project will comprise the following:

- Supply, delivery, commissioning and maintenance of four (4) Unmanned Aerial Vehicles (Drones)

Establishment of a command and control centre for surveillance, monitoring and analysis of Drone live feeds:

- Supply and installation of a command center for centralized monitoring of the drones
- Integration of the drones procured and live feed from all the drones
- Training of staff on use and maintenance of the Drones
- Maintenance and support of both the drones and all accessories

Schedule of Requirements

No.	Item	Sub-item	QTY
1	Command Centre	Power Supply, Lighting, Cooling system, 2 Servers, 10 work stations, 4 video walls, 2 routers, 2 switches, 10 phones/ intercom systems, 2 Printers/ scanners, operating system, specialized software, database management, security software, VPN, Data storage, Data Backup, 360 degrees/ omnidirectional cameras	1
2	UAV - Drones	UAV - Drones system complete with its accessories	4
4	Support and Maintenance	Maintain the UAV for a period of three (3) years Provide online support and license renewal for the three (3) years	3
5	Training & Knowledge Transfer	The successful provider will train three (3) personnel as pilots and two (2) personnel as maintenance crew at the factory	5

5. Methodology

The vendor should clearly demonstrate a comprehensive understanding of the Terms of Reference (TOR) and all outlined requirements for the supply, delivery, commissioning and maintenance of Unmanned Aerial Vehicles (Drones). In addition, they should present a well-defined delivery methodology that explains how they intend to execute the assignment.

6. Implementation team and responsibility

The vendor should clearly demonstrate the firm's overall experience, as well as present a detailed breakdown of the proposed team structure. This should include the qualifications, roles and relevant experience of all key experts who will be assigned to the assignment.

7. Implementation schedule work plan

Bidders shall propose an implementation schedule with clear milestones to which they will be contractually bound. The vendor is expected to complete the entire assignment within a maximum period of 18 months and a warranty period of one year.
The maintenance and support period is three years.

8. Expected Deliverables

- UAVs (Drones):
  - Patrol drones
  - Cameras systems on drones to capture images and videos.
  - Remote flight controllers, sensors and GPS.
- Improved Surveillance:
  - Real-time border patrol and surveillance images and videos.
- Data Integration and Sharing:
  - Integration with existing and future infrastructure.
- Reduced Processing Times:
  - Drones will reduce time to identify and resolve border infringements.
- Improved Border Management:
  - Optimized border management through drone patrols.
- Enhanced Data Accuracy:
  - Improved data integrity and reliability from videos and photos.

  - Video tracking of border patrol operations.
- Increased Revenue Collection:
  - Reduction of smuggling, which increases the amount of collected customs duties.
- Surveillance Systems:
  - Deployment of video cameras, sensors, and other surveillance equipment.
  - Implementation of video analytics and other advanced monitoring tools.
- Data Management Systems:
  - Development of centralized databases for data storage and analysis.
  - Implementation of data security and privacy measures.
- Standard Operating Procedures (SOPs):
  - Development of clear guidelines for the use of UAV (Drone) systems.
  - Establishment of protocols for responding to security incidents.
- Training Programs:
  - Training for customs officers and other support personnel on the use of drone technology.
- Maintenance and Support:
  - Provide Maintenance and support services for the UAV (Drone) systems.

9. Detailed Technical Specification/Requirements

PART A: TECHNICAL SPECIFICATION REQUIREMENTS

Instructions to Bidders:

1. Bidders MUST complete the Tables below in the format provided.
2. Bids MUST meet all mandatory (MUST) requirements in the Tables below in order to be considered for further evaluation.
3. Bidders MUST provide a substantial response or clear commitment to meeting the requirements for all features irrespective of any attached technical documents in the table format (bidders Response) below. Use of Yes, No, tick, compliant, blank spaces etc. will be considered non-responsive.
4. Bidders who do not comply with any of the below requirements will NOT be considered for further evaluation

A. FUNCTIONAL REQUIREMENTS

Functionality Requirements and Technical Requirements

Bidders are required to demonstrate how their proposed solution meets the listed requirements. Each requirement will be evaluated and scored according to the following criteria.

Table 1: Functional Requirements

S/No	Feature	Minimum Feature	Bidder's Response Pass/Fail
1.	Ground Control Station (GCS)	MIL-STD ruggedized touch screen laptop complete with a manual override handheld joystick for manual override and precision landing	
2.	The intelligent ISR drone	The drone should be capable of autonomous target tracking, automatic following, high-resolution on-board recording,	

		precise target positioning, Cursor on Target integration, and video-based position correction, up to 80 km range for single and dual operators.	
3.	Anti-jamming GNSS	Resists up to 7 active GPS jammers, using a CRPA System to provide jam-free GNSS signals or equivalent. Interference avoidance enabled S-Band radio upto 80km range	
4.	Stealth Switch system	A system that will allow full autonomous navigation without any radio emissions	
5.	Advanced Data Safety Software	Capable of preventing data disclosure of critical data even with physical access to the drone	
6.	Inertial navigation	Navigate accurately in GPS-denied environments. Uses inertial and vision-based navigation for position awareness, even during take-off and landing.	
7.	Interference avoidance	Highly resistant to Electronic Warfare interference using advanced interference avoidance radio systems and directional data links.	
8.	ATAK integration	Integrates ATAK standards for mesh collaboration with a vast range of military-grade ISR drone systems for insight and data sharing.	

9.	Remote Monitoring	Secured command centre integration-for real time monitoring	
10.	Flight modes supported	Full autonomous, manual override, point of interest, camera guided	

B. NON-FUNCTIONAL REQUIREMENTS

Bidders are required to demonstrate how their proposed solution meets the listed requirements. Each requirement will be evaluated and scored according to the following criteria.

Table 2: Non-Functional Requirements

No	Feature	Bidder's response
1.	**Usability**	
	The system should have a user-friendly dashboards and interfaces	
	The system should be scalable and adaptable to handle volumes and different environmental conditions	
	The system should allow an officer to generate, view and print customizable report(s).	
	System should provide an audit trail for all the surveillance conducted.	
2.	**Configuration Management**	
a)	The system should have the following capabilities:	
b)	Access control management	
c)	User role management with nomenclature of roles	
d)	Audit trail of any accesses or adjustments made to the system	
3.	**Integration Requirements**	
a)	The system should have an Application Programming Interface (API) that allows other systems to access and interact with its functionality and data.	
b)	The system should be able to integrate with existing authentication and authorization systems to enable single sign-on (SSO) for users.	
c)	The system should be able to import and export data in different formats, including XML, CSV, JSON, or other relevant file formats, to enable seamless data exchange with other systems.	
d)	The system should be able to integrate with databases used by other systems or applications, such as ICMS, RECTS	
e)	The system should be able to integrate with notification systems to alert users of important events or changes related to patrol/surveillance operations	

f)	The system should be able to integrate with web services to enable data exchange and communication between different systems or applications.	
4.	**Security**	
a)	Each user must be authenticated with a unique user-id and password on the application.	
b)	All user and account management changes and attempts must be logged	
c)	User authentication data must be stored and maintained securely in a centralized location on the system	
d)	The application must support password expiry features with a configurable frequency. Parameterize this to allow flexibility in adjusting this value as required.	
e)	The password must be secure on entry, at no point must the password be in clear text	
f)	All new user accounts must be created with reference to existing authoritative databases of approved persons e.g., identifying numbers in KRA's active staff database (HR)	
g)	All network communications between components must be authenticated, and must not explicitly trust other network devices	
h)	Systems directly facing the Internet must not store or cache confidential data, even for a short duration. This includes file uploads and downloads, source code, etc.	
i)	Applications must not connect to a database as a privileged user, such as the SA account in SQL Server or SYSTEM account in Oracle	
j)	Applications that connect to a database, application server, or any system that utilizes application IDs must do so using an account that has been granted access to only objects and functions needed for operation of the application	
k)	All servers should be kept in sync with a time synchronization mechanism. All communication sessions must use secure protocols	

l)	Any vendor proprietary protocols used must be well documented (i.e. the vendor must provide comprehensive documentation on the protocols such as technical specifications or white papers). Any vendor proprietary encryption algorithms must be FIPS-140 certified.	
m)	All relevant session information should be captured and stored in a secure & auditable location	
n)	System to implement automatic timeouts for user authentication to prevent unauthorized access in case a user leaves the session unattended	
o)	System to have the capability to promptly revoke access permissions when a user status changes or when a security breach is detected	
5.	**Other System Features**	
a)	Secure UAV and surveillance system operating platforms regularly monitored and prevented from system downtime, systems attacks	
b)	Audit trail for all functions executed through the UAV and surveillance system	
c)	System to be safe from data loss	
d)	System to be available in different devices including Windows, Android, IOS	
e)	Technology: The various components of the UAV and surveillance system to be from reputable internationally recognized brand, in existence for at least 5 years	
	Remarks – Pass / Fail	

Mandatory Minimum Technical Specifications

Table 3: Minimum technical specifications for the 4 Unmanned Aerial Vehicles – Drones.

S/No	Feature	Minimum Feature	Bidder's Response
A.	**Physical Features**		
	Wingspan	260-300cm	
	Length	70-120cm	
	Airframe material	Fiberglass, carbon, Kevlar, and composite	

	Landing Gear	Automatic landing gear retraction to provide 360° free field of view throughout mission execution.	
B.	**Weight and Payload**		
	Maximum take-off weight	9.0-14.0 Kg	
	Payload Capacity	3kg with single battery	
		1kg with dual battery	
C.	**Performance Features**		
1.	Take off & Landing	Vertical Take-off & Landing (VTOL)	
2.	Propulsion	Electric	
3.	Flight speed	Not less than 60 km/h	
4.	Air speed	Not less than 82km/h	
5.	Flight Time	Not less than 240 minutes	
6.	Flight Range	Not less than 240 Km	
7.	Radio Range	Up to 80 Km	
8.	Transmission Frequency	2.2-2.5 GHZ	
9.	GNSS System	L1/L2 GPS	
10.	Radio	2x2 MIMO	
		Interference avoidance licence	
		Non-rugged OEM	
		Bandwidth 20/10/5 MHz	
		Output power 10 watt	
		Rugged transport case	
		GPS based automatic vehicle tracking	
11.	Tolerances		
	i. Maximum takeoff/landing wind	45 Km/h	
	ii. Maximum wind cruise flight	50 Km/h	
	iii. Maximum precipitation	7 mm/h (Drizzle)	
	iv. Operating temperature	-20 and +45 Celsius	
	v. Maximum flight altitude AMSL	3500-5000 m	
12.	Ingress Protection	IP54	
13.	Transmission Frequency	2.4/5.0 Ghz AES encrypted	
D.	**Accessories**		

1.	Spare Propeller set	A set of 4 quadcopter propellers and one pusher motor propeller. The set should be balanced for optimal performance and free of vibration	
	Batteries	4 flight batteries	
2.		Dual battery charger	
3.		Auxiliary battery mount	
4.	Flight case	1 ruggedized transport case	
E.	**Surveillance Sensor: EO/IR**		
1.	Visible Camera	Visible 400-700 nm	
2.		Resolution: 1280x720	
3.		Zoom: x40+x2 digital, (total x80) continuous zoom	
4.		HFOV:60°WFOV-1.5°NFOV-0.75°DFOV	
5.	Thermal Camera	LWIR uncooled (8-14 µm)	
		Resolution: 1280x720	
		Zoom: X8 digital, continuous zoom	
		HFOV:17.5°W.FOV-2.2°NFOV-0.75°DFOV	
		Weight:≤1 kg	
		Temperature:20°C to +55°C	
6.	Field of Regard	Pan: 360° continuous	
7.	Power Consumption	Typical 7-12 W	
8.	Video Compression: H264		
9.	GPS controlled camera position holding		
10.	Camera automatically tracks objects		
11.	Pan, Tilt & 40x zoom control		
12.	UAV can autonomously follow objects that are being tracked		
13.	On-board Video Recording & Snapshots: 64 Gb on-board memory		
14.	Camera retraction mechanism: Deploy and retract the camera inside the fuselage automatically during take-off and landing		
	Johnson's criteria-DRI Ranges Visible Channel		
15.	Man		
16.	Detect	>10 km	
17.	Recognize	>6km	
18.	Identify	>3km	
19.	Vehicle		
20.	Detect	>40 km	
21.	Recognize	>1km	

22.	Identify	>6km	
	Johnson's criteria-DRI Ranges Thermal Channel		
23.	Man		
24.	Detect	>3 km	
25.	Recognize	>1 km	
26.	Identify	>500 m	
27.	Vehicle		
28.	Detect	>4 km	
29.	Recognize	>1700m	
30.	Identify	>850m	
F.	**Training**		
1.	Training of Pilots	The successful provider will train three (3) personnel as pilots and two (2) personnel as maintenance crew at the factory	
G.	**Maintenance**		
1.	Maintenance	The successful provider will, 1.Maintain the UAV for a period of three (3) years 2.Provide online support and license renewal for the three (3) years	
H.	**Warranty**		
1.	Warranty	The successful provider will give warranty for the UAV for a period of 1 year	
I.	**Ruggedized Video Control Station Laptop**	Quantity-2	
1.	The Ground Control Station (GCS) should be a MIL-STD ruggedized touch screen laptop complete with manual override handheld joystick		
2.	Intel® Core™ i7 1145G7 vPro™ Processor or equivalent		
3.	Windows 10 Pro 64-bit or equivalent		
4.	16 GB DDR4 RAM (max.64GB)		
5.	Intel® UHD Graphics, support Intel® Iris® Xe Graphics when 2 RAM Modules installed		
6.	512 GB NVMe Opal SSD		
7.	14" Active Matrix (TFT) colour LCD 1920 x 1080 pixels (Full-HD), capacitive 10 finger Touch Screen		
8.	Wireless Lan	Intel® Wi-Fi6 AX201	
9.	Mobile Broadband	Intel® Wi-Fi6 AX201	

10.	Global Positioning	u-blox NEO-M8N (supports GPS, GLONASS, Beidou, Galileo)	
11.	Battery	Lithium-Ion 10.8V, 6500mAh (typ) 6300mAh (min.)	
12.	Battery Life	1st Battery-Approx 5 hours 2nd Battery- Approx 12-15 hours	
13.	Hot Swap	With the second Battery	

Table 4: Minimum technical specifications of communication and networking

No.	Feature	Minimum Requirements	Bidder's Response
1	Network Interfaces	• **Ethernet**: 10/100/1000 Mbps • **Wi-Fi**: IEEE 802.11a/b/g/n/ac • **Bluetooth**: Version 4.0 or higher	
2	Protocols	• **TCP/IP**: For network communication • **HTTPS**: For secure web-based management • **SNMP**: For network management and monitoring	

Table 5: Minimum technical specifications of software and integration

No.	Feature	Minimum Requirements	Bidder's Response
1	Operating System	• **Embedded OS**: Linux-based or custom real-time OS	
2	Access Control Software	• **Features**: User management, real-time monitoring, reporting, integration with other security systems	

No.	Feature	Minimum Requirements	Bidder's Response
		• **Database**: SQL-based, support for distributed architecture	
3	API Integration	• **Restful API**: For third-party integrations • **SDKs**: Available for various programming languages (Java, C#, Python)	

Table 6: Minimum technical specifications of security and encryption

No.	Feature	Minimum Requirements	Bidder's Response Pass/Fail
1	Data Encryption	• **Methods**: AES-256 for data storage, TLS 1.2/1.3 for data transmission	
2	User Authentication	• **Multi-Factor Authentication (MFA)**: Support for combining RFID, biometrics, and PINs	
3	Tamper Detection	• **Sensors**: Embedded tamper switches and accelerometers	

Table 7: Minimum technical specifications of maintenance and support

No.	Feature	Minimum Requirements	Bidder's Response
1	Remote Management	• **Capabilities**: Remote diagnostics, firmware updates, and configuration	
2	Warranty and Support	• **Warranty**: Typically, up to 1 year • **Support**: 24/7 technical support,	

		on-site maintenance options.	

Table 8: Minimum technical camera – Video/Image management software (VMS)

No.	Feature	Minimum Requirements	Bidder's Response
1	**Features**	• **Live View**: Real-time monitoring of multiple camera feeds • **Playback**: Search and playback recorded footage • **Alerts**: Motion detection, tampering alerts, analytics-based alerts • **User Management**: Role-based access control	
2	**Analytics**	• **Basic**: Motion detection, line crossing, intrusion detection • **Advanced**: Facial recognition, image recognition, object tracking, heat mapping	
3	**Integration**	• **Access Control Systems**: Integration with existing access control for comprehensive security • **Alarm Systems**: Integration with fire and security alarms	
4	**Interface**	• **Web-Based**: Accessible through web browsers • **Desktop Application**: Windows, MacOS • **Mobile Application**: iOS, Android	

Table 9: Minimum technical specifications and bills of quantities of items for 1 (1) centralized command center.

NO.	ITEM	SPECIFICATION	QTY	Bidder's response
1.	Inspection Supervision Station (Image Processing Work Station CPU)	CPU: Xeon E5-1620 v3 (4 cores, 3.5GHz 10M), Memory: 16GB DDR4, Hard disk: 500GB SATA3 7200RPM, Optical drive: DVD+/-RW, Power supply: 685W, USB keyboard (English) + Optical mouse. Installed with Kaspersky antivirus	10	
2.	Displays	98 inches, 8K UHD (7680 x 4320), **High Brightness:** 700 to 2500 nits or higher for video walls, High contrast ratios (3000:1 and above), Wide viewing angles (178°/178°), Support for wide color gamuts (e.g., sRGB, Adobe RGB, DCI-P3)	4	
3.	Routers	Wireless Standards802.11ax (Wi-Fi 6)802.11be (Wi-Fi 7)Speed(e.g., 600 Mbps on 2.4 GHz, 1300 Mbps on 5 GHz)RAM (e.g., 256MB, 512MB, 1GB)Ethernet Ports: Number of LAN (usually 4-8) and WAN (1)USB Ports: USB 2.0 and 3.0	2	
4.	Switches	Cisco Catalyst 2960-X Series: Ubiquiti UniFi Switch	2	
5.	Graphics card	Interface: PCI-E 3.0 GPU: NVIDIA Geforce GTX 1050 Ti Memory: 4G, DDR5, 128bit 3D API: DirectX supports up to 12.1 Interface: DVI*1, HDMI*1, DP*1 Maximum resolution: 2560×1600 Recommended power: 300W or more	10	
6.	Workstation Monitor	32 inch flat-screen display Resolution: 2560*1440 Interface: DP & HDMI & VGA	10	

		Stand: Flexible stand with capability to: Adjust height, rotate on horizontal axis, and rotate on vertical axis		
7.	UPS (for workstation)	1000w	10	
8.	UPS (for workstation)	8000w	2	
9.	Operating System (for workstation)	Windows 10 IOT Enterprise 2016 LTSB 64-bit English version	10	
10.	Network Switch (Po)E	48 Port POE Switch, 48x10/100/1000Base-T Ethernet ports (PoE), 4x1000Base-X SFP Ethernet ports	2	
11.	NVR	320mbps 12 million pixels, maximum, h.265 1080P decoding circuit, VGA, HDMI 1 1/2 Gigabit RJ45 interface, 2usb3.0 1CH), 1/audio input/output, support 8 bays (6TB per hard disk), 1 eSATA, 16 / 6 alarm interface input / output, P2P, fisheye dewarp, face detection, RAID0 / 1 / 5 / 6 / 10	4	
12.	LED TV	85", Wall Mount Bracket	4	
13.	Splicing Screen	46" splicing screen and accessories for installation	10	
14.	Fish eye camera	See the included minimum specifications	2	
15.	Cabinet	600 x 1000 x 205542U, Black Colour	1	
16.	Dimensions	Command centre – 30 by 15 metres Equipment room 4 by 4 metres	1	
17.	Accessories	Network Cable, Network Registered Jack (RJ-45, Cat5E), DVI Monitor Cable, PDU power for cabinets	1	
18.	Image analysis software	Tailor Made for KRA image analysis	For 10 CPUs	

19.	Other Items, Accessories, etc. necessary to operationalize the command centre	List all the other Items and Accessories necessary to operationalize the command centre	LOT	
	Furniture			
20.	Lockable compartments	Pigeon-Hole Lockout Box Storage System	10 lockable compartments	
21.	Command Centre Desks	Standard command centre desks	15	
22.	Command Centre Chairs	Orthopaedic chairs	15	
23.	Fridge	STANDARD 210LTRS DOUBLE DOOR FRIDGE- RT26HAR2DSA FEATURES: • 210 Litres Capacity • Net Dimensions: 56cm(W) x 63cm(D) x 145cm(H) • Digital Inverter Compressor with a 20 Year Warranty • Multi flow Air System • LED Lighting • Easy Slide Shelf • Cool Pack – up to 8 hours • In-built Power Stabilizer • No Frost Technology • Big Door Guard • Easy Space Manager • Tempered Glass Shelves • Silver Technology Deodorizer • Recessed Easy Handle • Multi Storage Basket • 5 Star Energy Rating • Colour: Silver/black	2	

Table 10: High Level Security Requirements

No	Feature	Requirement	Bidder's detailed Response
1	Data Encryption	All data, both at rest and in transit, must be encrypted using industry-standard encryption algorithms to prevent unauthorized access. Any vendor proprietary encryption algorithm must be FIPS-140 certified.	
2	Access Control	The system must implement robust access control mechanisms, including multi-factor authentication, role-based access controls, and the principle of least privilege.	
3	Auditing and Logging	Comprehensive audit trails must be maintained for all system activities, enabling traceability and accountability. Ensure the logs are in a format that is consumable by Security information and event management (SIEM) system.	
4	Incident Response	An effective incident response plan must be established by the vendor to address security breaches or incidents promptly and minimize impact.	
5	Data Integrity	Mechanisms must be in place to ensure the integrity of data, including checksums, digital signatures, and block chain technology where applicable.	
6	Continuous Monitoring	The system must have continuous monitoring capabilities to detect and respond to security threats in real-time.	
7	Security Training	Vendors must provide security training for system users and administrators to foster a culture of security awareness.	
8	Secure Development	The solution must be developed following secure coding practices, and vendors must demonstrate a commitment to security throughout the software development lifecycle.	
9	Authentication	No identification and authentication information must be hard-coded or scripted into the application.	

10	Compliance to Detailed KRA Security Requirements	The solution must be implemented in compliance with the detailed KRA Application Security requirements (Annex III) and API Security requirements (Annex IV). The detailed requirements will form part of the Information Security test cases.	

Vendor Evaluation

	Bidder Experience	**Maximum score**
No.	**Requirement Description**	
1.	**<u>Firm's Experience</u>** At least Three (3) years' Experience in Supply, delivery, commissioning and maintenance of Unmanned Aerial Vehicles - Drones. The bidder to provide a Company profile demonstrating ability to Supply, Deliver, Commission and respond to all maintenance issues. **(*3 marks*)** Certificate of Incorporation: Above Five (5) years…**(2 *marks*)** Certificate of Incorporation: 3-5 years…… **(1 marks)** Bidder is required to describe and provide evidence of **three (3) similar projects** the bidder has undertaken within the last 5 years: a) Contract or LSO; b) Completion certificate or Reference/recommendation letter from client For each satisfactory reference, the bidder will be scored per areas listed above: **i)** Contracts or Service Orders **(1 Mark per client),** ii) Completion certificate or Recommendation letter from client **(2 mark per client)** References required should be for sites where the bidder or its partners in the project implemented solution.	11
2.	**Project Team**	
	<u>Personnel's Qualifications and Experience</u> Bidder is required to provide a responsibility matrix and profiles of delivery leads (**Project Manager, Development Lead, Solution Architecture Lead, and Infrastructure Lead**). Bidders are required to submit actual and current project team members of the core team expected to be involved in the project and clearly indicating where the teams have carried out similar implementations. Bidders must	24

	provide the following documents for the core team: a) Detailed CV b) Academic qualifications/certificates c) Years of experience d) Relevant certifications	
	For each lead the scoring will be as follows: (**Project Manager, Engineering Lead, Solution Architecture Lead, Infrastructure Lead – 4 Leads to be evaluated)** **Project Manager** a) Lead (Project Manager) i. Degree in Electronic Engineering, Electrical Engineering, Telecommunications, Computer science, ICT or other related field **(2 Marks)** (attach certificate) ii. Diploma in Electronic Engineering, Electrical Engineering, Telecommunications, Computer science, ICT or other related field **(1 Mark)** (attach certificate) b) Certification in Project Management (PMP/ Prince2) or any other similar/related course. (Must attach copy of certificate) – **2 marks** c) Must have a minimum of five (5) years' experience in Project Management (Must provide detailed and signed CV) i. 5 years and above – **2 marks** ii. Below 5 years – **0 mark**	6
	Engineering Lead a) Lead with relevant qualification i. Degree in Electronic Engineering, Electrical Engineering, Telecommunications, Computer science, ICT or other related engineering field **(2 Marks)** (attach certificate) ii. Diploma in Electronic Engineering, Electrical Engineering, Telecommunications, Computer science, ICT or other related engineering field **(1 Mark)** (attach certificate) b) Certification in Project Management (PMP/Prince2) or any other similar/related course. (Must attach copy of certificate) – **2 marks** c) Must have a minimum of five (5) years' experience in Engineering (Must provide detailed and signed CV) i. 5 years and above – **2 marks** ii. Below 5 years – **0 mark**	6

	Solution Architecture Lead a) Lead with relevant qualification i. Degree in Electronic Engineering, Electrical Engineering, Telecommunications, Computer science, ICT or other related field **(2 Marks)** (attach certificate) ii. Diploma in Electronic Engineering, Electrical Engineering, Telecommunications, Computer science, ICT or other related field **(1 Mark)** (attach certificate) b) The Lead must have certification in Project Management (PMP/Prince2) or any other similar/related course. (Must attach copy of certificate) **– 2 marks** c) Must have a minimum of five (5) years' experience in solution architecture (Must provide detailed and signed CV) i. 5 years and above – **2 marks** ii. Below 5 years – **0 mark**	6
	Infrastructure/Aviation Lead a) Lead with relevant qualification i. Degree in Electronic Engineering, Electrical Engineering, Telecommunications, Computer science, ICT or other related field **(2 Marks)** (attach certificate) ii. Diploma in Electronic Engineering, Electrical Engineering, Telecommunications, Computer science, ICT or other related field **(1 Mark)** (attach certificate) **b)** The Lead must have certification in Project Management (PMP/Prince2) or any other similar/related course. (Must attach copy of certificate) **– 2 marks** c) Must have a minimum of five (5) years' experience in IT infrastructure/Aviation (Must provide detailed and signed CV) i. 5 years and above – **2 marks** ii. Below 5 years – **0 mark**	6
	Adequacy of the proposed Methodology and Work Plan in responding to the Terms of Reference will be evaluated on how the consultant proposes to address the areas listed below	

	Supply, delivery, commissioning and maintenance of Unmanned Aerial Vehicles - Drones In this section the bidder is expected to provide a detailed and comprehensive work plan and methodology(s) on how they intend to execute the items indicated below (Starting second bullet) • Development of detailed Work plan with specific and clear milestones **(2 Marks)** • Supply, delivery, commissioning and maintenance of Four (4) Unmanned Aerial Vehicles - Drones Kenya **(7 marks)** • Establishment of 1 command and control center for surveillance and analysis and monitoring of Drones live feeds **(5 marks)** • Integration of the command center with other KRA systems **(3 marks)** • Training of staff on UAV's use and surveillance **(1 mark)** Maintenance and support of the UAV's and infrastructure **(2 marks)**	20
	Total Score = 55 **Cut-off Score = 44**	**55**

10. DEMO

Bidders who are successful in the Technical Requirements will be invited for a live presentation/demo that will form additional assessment of the Drones capabilities and vendor experience.

The Components of the presentation/demo to broadly include:

i) The vendor should provide a comprehensive demonstration that highlights the Drone's functionality, security, and convenience features. The Demo should showcase working Drones with its various components, e.g, GCS, Cameras and command center.

The vendor should also show case surveillance cameras capable of character recognition/thermal imaging, high quality video and resolution, transmission to the command center and Integration to existing platforms

	Component	Requirement	Expected output	Max Score	Score
1.	Access Control Mechanisms	How the Drones grants or denies access, including keypads, biometric scanners, and mobile app integration.	Time taken to grant/deny access	2	
2.	Sensors and Alarms	The types of sensors used on the cameras, such as motion detectors, and how they contribute to security and convenience.	Trigger mechanism for images	2	
3.	Drone operation	The operation of the drone, its speed, noise level, and the mechanical parts that ensure smooth operation of the drone	Reliability and Sustainability of drones	2	
4.	Intercom System	Demonstrating communication will be done between ground operation crew and the command centre.	Enhanced communication	2	
5.	Image Integration	Showcasing any cameras that are part of the drones, their resolution, night vision capabilities, and how they integrate with recording systems.	Quality of Image/video feed capture Cloud connectivity	2	
6.	Safety Features	Demonstrating safety features on the drones that will prevent collisions and crashing.	Warning signs, sirens, manual override	1	
7.	Integration with Smart Systems	How the drones can integrate with other smart systems for a seamless automation experience.	Ease of data exchange	1	
8.	Weight and Dimensions Control	Demonstrate weight and dimensions of the drone	Weight and dimension measurements	2	
9.	Camera Housing	Demonstrating the durability and protective features of the camera's housing	Durability and protection from weather elements	1	
10.	Lens	The quality of the lens affects image clarity, and vendors can demonstrate different types such as fixed-focus and zoom lenses	High Image Quality (4K)	1	

11.	Processor	The processor should convert signals into digital images in real time and transmit to Command center.	Speed of transmission	1	
12.	Storage	Showing the options for video storage, whether it's built-in or external like an SD card or cloud storage	Internal or external storage	1	
13.	Power Supply	Power requirements and options like Power over Ethernet (PoE) for convenience	AC power or DC power	1	
14.	Networking Interface	Presenting the camera's networking capabilities for transmitting images and enabling remote monitoring and viewing	Wireless, Wired or Power over Ethernet (PoE)	1	
15.	User Interface	A system that allows configuration, live viewing and analytics, through a web browser. A system that provides advanced features and monitoring capabilities. A system that enables control through a smartphone.	Web Interface, desktop software or mobile application	1	
	Total Score = 21 **Cutoff score = 15**			**21**	

11. Financial proposal form

No.	Item	Sub-item	QTY	UNIT COST (KSH)	TOTAL COST (KSH) Taxes inclusive
1	Command Centre	Power Supply, Lighting, Cooling system, 2 Servers, 10 work stations, 4 video walls, 2 routers, 2 switches, 10 phones/ intercom systems, 2 Printers/ scanners, operating system, specialized software, database management, security software, VPN, Data storage, Data Backup, 360 degrees/ omnidirectional cameras	1		
2	UAV - Drones	UAV - Drones system complete with all its accessories	4		
4	Support and Maintenance	1. Maintain the UAV for a period of three (3) years 2. Provide online support and license renewal for the three (3) years	3		
5	Training & Knowledge Transfer	The successful provider will train three (3) personnel as pilots and two (2) personnel as maintenance crew at the factory	1		
Grand Total Cost –To be carried Forward to the Form of Tender					

OVERALL EVALUATION

The bid evaluation will take into account technical factors in addition to cost factors. The weight for Technical evaluation is 80% while Financial Evaluation will be based on the Lowest Evaluated Bid.

SUMMARY OF THE EVALUATION SCORES

Criteria	Maximum Score / Requirement	Cut-off Score
Technical requirements/Specifications and	**Mandatory**	**Met**
Bidder Qualifications (Vendor) and Methodology	**55**	**44**
Demo	**21**	**15**

Notes

1. The quoted price shall be in Kenyan shillings encompassing all costs associated with the Project scope of work. Additionally, it shall cover maintenance services, transfer of knowledge, and acquisition of the any source code. All these elements are to be included within the total quoted price without any additional charges.
2. The financial remuneration for the supply, delivery, commissioning and maintenance of Unmanned Aerial Vehicles (Drones) will adhere to the following terms:
   Milestone-Based Payments: At the negotiation stage payment shall be structured around the successful completion of predefined milestones that correspond to the project's phases. Each milestone payment will be contingent upon the acceptance of deliverables as per the agreed-upon specifications and timelines.

Annex II API Security Requirements

General Rule: The solution must implement API-first design for integration i.e. API-first design for integration is a development strategy where APIs are designed, documented and defined before any application code is written, treating the API as a core product, not an afterthought.	
	ANNEX I - API Security Requirements
	Review Area
1	**Governance**
1.1	Ensure the API is properly versioned. Versioning helps in keeping track and maintenance of the API.
1.2	Ensure that the API conforms to the organization set style and design guidelines such formatting of headers for consistency.
1.3	Ensure that the API is included as part of the organization's APIs inventory for Discoverability and Reusability
2	**Authentication**
2.1	Ensure that every request to the API or web service is authenticated.
2.2	Ensure a strong authentication mechanism is used; Required authentication mechanisms allowed for APIs/Web services in KRA are OAuth 2.0 and JWT
2.4	Ensure implementation of anti-brute force mechanisms on authentication endpoints such as account lock-outs, use Max Retry and jail features in Login.
2.6	When JWT is used, ensure: 1. Use a random complicated key (JWT Secret) to make brute forcing the token very hard. 2. Don't extract the algorithm from the header. Force the algorithm in the backend (HS256 or RS256). 3. Make token expiration (TTL, RTTL) as short as possible. 4. Don't store sensitive data in the JWT payload, it can be decoded easily.
2.7	When OAuth 2.0, ensure: 1. Always validate redirect_uri server-side to allow only whitelisted URLs. 2. Always try to exchange for code and not tokens (don't allow response type=token). 3. Use state parameter with a random hash to prevent CSRF on the OAuth authentication process. 4. Define the default scope, and validate scope parameters for each application.

2.8	Ensure no sensitive authentication details, such as auth tokens and passwords are sent in the URL through GET requests.
3	**Authorization**
3.1	Ensure a proper authorization mechanism is implemented that checks if the authenticated subject has access to perform the requested action.
3.2	Ensure that the issued authentication and authorization tokens have a set expiry time.
3.3	Ensure the use of random and unpredictable values as Globally Unique Identifiers (GUIDs) for records identification. Auto-incrementing IDs should never be used.
3.4	Ensure the use of proper HTTP method for each API operation: GET (read), POST (create), DELETE (to delete a record). No request should be processed if the method is not appropriate for the requested resource.
3.5	Ensure the integrating components only access the objects they require from the integrating systems. Responses should only return the data necessary to fulfil a request
4	**Data Protection**
4.1	Ensure that the responses from the API provide only legitimate requested data that is not excessive.
4.2	Ensure sensitive information such as access tokens, bearer tokens, pins, passwords etc are not being returned in request responses or stored in logs in clear text.
4.3	Error messages must ensure that sensitive information about the integrating systems is not disclosed
4.4	Ensure sensitive data parameters such as passwords, PINs, Credit card numbers etc. being passed to the APIs are hashed
4.5	Ensure minimization/masking of customer PII such as MSISDN and ID Numbers when such are returned in request responses and displayed in logs.
4.6	Ensure the communication channel is encrypted. The Endpoints should make use of HTTPS and not of HTTP
4.7	Ensure proper implementation of HTTPS; i.e current secure TLSV
5	**Resource and Rate Limiting**
5.1	Ensure implementation of a limit on how often a client can call the API within a defined timeframe. This helps mitigate DoS attacks by throttling or blocking IP addresses after making concurrent requests within a very short period of time.
5.2	Define and enforce maximum size of data on all incoming parameters and payloads such as maximum length for strings and maximum number of elements in arrays.

5.3	For APIs processing large amounts of data, ensure data is processed asynchronously. Processing large amounts of data synchronously can prevent the API from responding in a timely manner forcing clients to wait.
6	**Secure Configuration**
6.1	Ensure implementation of the **X-Content-Type-Options: nosniff** header to protect API against MIME sniffing vulnerabilities.
6.2	Ensure implementation of the **X-Frame-Options: deny** header.
6.3	Ensure implementation of the **Content-Security-Policy: default-src 'none'** header.
6.4	Ensure that fingerprinting headers such as **X-Powered-By**, **Server**, **X-AspNet-Version**, etc are not present
6.5	Force content-type for your response. If you return application/json, then your content-type response is application/json.
6.6	Return the proper status code according to the operation completed. (e.g. 200 OK, 400 Bad Request, 401 Unauthorized, 405 Method Not Allowed, etc.).
7	**Vulnerability Management**
7.1	Ensure that the API supports use of updated and vendor supported dependencies and libraries.
7.2	If the API is externally facing, ensure that it's behind a Firewall
7.3	Ensure that unused dependencies, unnecessary features, components, files, and documentation are deleted in production APIs
8	**Data/Input Validation**
8.1	Perform data validation using a single, trustworthy and actively maintained library.
8.2	Validate, filter and sanitize all client-provided data, or other data coming from integrated systems.
8.3	Special characters should be escaped using the specific syntax for the target interpreter.
8.4	Prefer a safe API that provides a parameterized interface.
8.5	Always limit the number of returned records to prevent mass disclosure in case of injection.
8.6	Validate incoming data using sufficient filters to only allow valid values for each input parameter.
8.7	Define data types and strict patterns for all string parameters.
9	**Auditing and Logging**
9.1	Log all failed authentication attempts, denied access, input validation errors and rate limit errors
9.2	Ensure all requests and responses are logged

9.3	Ensure the logs are in a format that is consumable by SIEM systems
9.4	Ensure the log contains sufficient details including the actual source IP instead of a Load balanced IP in cases where the service is hosted behind a load balancer.
9.5	Ensure both the raw http access logs as well as the transactional logs are sent to a SIEM
9.6	Based on the functionality provided by the API define use cases for monitoring at the SOC
9.7	A facility should exist to allow Manual triggering of transactions/actions under special circumstances (eg Integration breakdown, compromise etc) There must be audit trail on the facility
10	**Network controls**
10.1	All network communications between integrating components must be authenticated, and must not explicitly trust other network devices
10.2	API's must not connect to a database as a privileged user, such as the SA account in SQL Server or SYSTEM account in Oracle
10.3	All function calls between applications should implement digital signatures to verify authenticity of the invoking application (eg tokens, SSL)
11	**Encryption**
11.1	API Authenticating tokens must be random and unpredictable
11.2	Data sent between integrating systems must be encrypted in transit. Recommended algorithms (with minimum bit lengths), in order of preference, are: Hashing: SHA -512, SHA -256, RIPEMD160. Symmetric: AES256, AES192, AES128, 3 -DES (168 bits), Blowfish(minimum 128 bits), Twofish (minimum 128 bits), IDEA (128 bits),and RC4 (128 its). Public key: RSA(minimum 2048 bits) and DSA(minimum 2048 bits), ElGamal (minimum 2048 bits)
11.3	Encryption keys must be protected during transit and while stored in file system
11.4	A key used to decrypt data must not be stored in the same location as data encrypted with the key
11.5	Site certificates must be current and issued by a well-known certificate authority
12	**Documentation**
12.1	A design blue print with data flow or flow chart diagrams should be present as part of the integrating application system/module/component documentations
12.2	Signed user requirements/specifications document should be present as it forms the basis for the development of a new application or modification of an existing system

Annex III: Application Security Requirements

	ANNEX II - Application Security Requirements
1	**Application Architecture**
1.1	Applications hosted in a shared hosting environment should be logically isolated from other applications in the same environment
1.2	Anti-virus scanning must be performed real-time on any file transmitted to the server
1.3	All network communications between components must be authenticated, and must not explicitly trust other network devices
1.4	If an application stores highly confidential information, data must be physically separated from other applications' data stores
1.5	Applications handling highly confidential data must not be hosted in a shared hosting environment or store its data in a shared database server
1.6	If an application shares a data store with another application, the data store must be segmented logically or physically. Logical segmentation should be implemented with access control mechanisms. Physical segmentation should be accomplished with a separate instance of the data store or a separate data store server
1.7	Any administrative functions that are not meant to be accessed by users from the Internet must be located in a private DMZ, which prevents direct Internet access to the servers
1.8	Systems directly facing the Internet must not store or cache confidential data, even for a short duration. This includes file uploads and downloads, source code, etc
1.9	Internet-facing systems must be placed behind a firewall that protects against network-based denial of service attacks, blocks ports that are not required for external access, and other network attacks
1.1	Applications must not connect to a database as a privileged user, such as the SA account in SQL Server or SYSTEM account in Oracle
1.11	Applications that connect to a database, application server, or any system that utilizes application IDs must do so using an account that has been granted access to only objects and functions needed for operation of the application
1.12	All function calls between application tiers should implement digital signatures to verify authenticity of the invoking application
1.13	Applications must be designed to enforce the least privilege principle for all processes

1.14	Application server interfaces must not be accessible from the Internet. This includes Web Services, DCOM, CORBA, SOAP, EJB, RPC, and any other method of invoking remote procedure calls
1.15	All application resources must require authentication for every call to each resource, and must be kept in compliance with the recommended password policies
1.16	All servers should be kept in sync with a time synchronization mechanism
2	**Network Communication and Session Management**
2.1	Sensitive information must be transmitted via a secure channel (SSL, SSH, etc.) or encrypted prior to transmission (PGP, etc.), using KRA approved methods
2.2	All communication sessions must use secure protocols
2.3	All transactions communication sessions must enforce session expiry so that after an unacceptable period of inactivity the session must terminate to guard against session hijacking
2.4	Any vendor proprietary protocols used must be well documented (i.e. the vendor must provide comprehensive documentation on the protocols such as technical specifications or white papers). Any vendor proprietary encryption algorithms must be FIPS-140 certified
2.5	Session IDs must use strong, non -predictable algorithms
2.6	All relevant session information should be captured and stored in a secure & auditable location
2.7	Only one session should be allowed per user operating from a single computer unless a specific business case has been established for allowing multiple sessions per user
2.8	Sessions should expire after a maximum set duration, regardless of activity
2.9	Session state must be maintained on the server for web-based applications, and be associated with a single client through the use of a session ID
2.1	Session state must be tied to a specific browser session through the use of a session cookie
2.11	Sessions must not be allowed to span both secure and non-secure connections
2.12	Applications must allocate session-based resources only after successful authentication. Allocating resources prior to this can lead to denial of service attacks, session fixation attacks, and others
2.13	Synchronization of time between servers and other relevant equipment must be implemented. This is instrumental in tracking time stamps between different systems particularly where systems share/exchange data
3	**Identification and Authentication**
3.1	Each user must be authenticated with a unique user-id and password on the application

3.2	User authentication data must be stored and maintained securely in a centralized location on the system
3.3	The application must support password expiry features with a configurable frequency. Parameterize this to allow flexibility in adjusting this value as required
3.4	The password must be secure on entry, at no point must the password be in clear text
3.5	All new user accounts must have a system-generated random password when created. A secure way of communicating the initial password to the user should be utilized e.g. via KRA e-mail account
3.6	All new user accounts must be created with reference to existing authoritative databases of approved persons e.g. identifying numbers in KRA's active staff database (HR) and National PIN certificate database
3.7	Users must be prompted to change their passwords the first time they log on to the application
3.8	Newly created accounts should be set to expire if not used for a configurable period of time. Parameterize this to allow flexibility in adjusting this value as required
3.9	The application must support password lockout after a configurable number of unsuccessful attempts. Parameterize this to allow flexibility in adjusting this value as required
3.1	The application must lockout a user account after the system is idle for a configurable period of time. Parameterize this to allow flexibility in adjusting this value as required
3.11	The application must support a password change notification and a configurable number of grace logins
3.12	The application must support the ability to disable / remove / delete a user, after a number of days of inactivity, the number of days should be configurable
3.13	The application must not allow the re-use of a past password until a set number of password changes have been made. Parameterize this to allow flexibility in adjusting this value as required
3.14	The application must be flexible and enforce a minimum password length of 8 characters
3.15	The application must enforce the usage of strong alphanumeric passwords
3.16	Default / developer passwords should not reside within the application
3.17	No identification and authentication information must be hard-coded or scripted into the application
3.18	The application must provide last logon information
3.19	Backward process flows must clear all authentication fields
3.2	The application must support time-based access control

3.21	Login failure measures must not indicate which component of the username/password pair submitted was incorrect
3.22	During password changes the application must force the user to enter the new password twice
3.23	The application must support Multi Factor Authentication with at least 3 factors to choose from (OTP, TOTP, Mail)
3.24	The application should support Single Sign On at a minimum through Identity Directories for Non-Revenue systems
4	**Authorization and Access Control**
4.1	The application must support an additive access model which means by default no access is granted
4.2	Access control must be granular to facilitate adequate separation of duties, for example:
	· There should be separation of duties e.g. data entry, authorisation and final approval
	· Data entry staff should have the minimum access levels required to enter data
	· Authorisation staff should have an access level that allows them to authorise but not necessarily change the data that was entered
	· Final approval staff should have the required access level to finalise the process/transaction
4.3	Access control information should be securely stored and must be secure from unauthorized changes within and outside of the application
4.4	Reporting on all the access permissions per user must be available in the application
4.5	User must be able to explicitly terminate (logout) a session
5	**Operations**
5.1	Intrusion detection systems must be in place to detect intrusions of production systems that are Internet facing
5.2	Patch management software must be installed and regularly updated on all servers
5.3	Anti-virus software must be installed and regularly updated on all servers
5.4	A formal incidence response process plan should be in place for production systems
6	**Auditing and Monitoring**
6.1	Provision must be in place for application logs
6.2	All application logs must be in a user-friendly readable format and in English
	They should be delimited using space and allow activities to be captured per line of text Each user transaction such as printing, viewing, updates, inserts and other data manipulation should capture to the minimum the date and time, userID, the URL accessed the and source IP & remote IP. They should indicate the parameters passed where possible

6.3	All application logs must be secure from intentional or accidental modification under all circumstances by all users including administrators. Access to the logs must be restricted to authorized users only so as to ensure their integrity
6.4	It should NOT be possible for the Application Audit logs to be suppressed or modified
6.5	All logs must be viewable and printable
6.6	The application must have incident alerting capability e.g. in the event of system violations or when the audit logs are getting full
6.7	All utility or non-standard based access to the application must be captured in the logs
6.8	For all application audit logs, the log files must bear the following information:
	a) User-id
	b) Date & Time of event
	c) The source and remote IP
	d) Type of event / action performed by the user
	e) Module accessed by the user
	f) Success or failure of the event
	g) Source of the event
	h) Before and after values (where applicable, i.e. master files)
	i) Modifications to the application
	j) Account creation, lockouts, modification, or deletion
	k) Modifications of privileges and access controls
	l) Application alerts and error messages
	m) Accesses to sensitive information
	n) URL of the web page(s) accessed by a user for Internet facing applications
	o) Program used to access the system
	p) The userID at the application log should be tracked up to the database logs
6.9	The application must have a logging mechanism to log all transactions and exceptions
6.1	A violation log must exist to track any attempted unauthorized access to the application and should bear the following information:
	a) Particular action intended by the user
	b) Workstation-id or IP address of access
	c) Date & Time of event

6.11	All valid and failed login attempts must be logged with meaningful information that is actionable for investigative purposes if fraud is detected. However, passwords must not be logged
6.12	All password recovery reset attempts must be logged with meaningful information that is actionable for investigative purposes if fraud is detected
6.13	All security policy changes and attempts must be logged
6.14	All user and account management changes and attempts must be logged
6.15	Database audit trails should be present for all dynamic & static tables of interest e.g. Parameter tables, Transaction Tables etc.
6.16	Application logs should be implemented independent of database audit trails for purposes of correlation i.e. application servers should maintain their own application logs separate from database audit trails.
7	**Input – Processing – Output Controls**
7.1	Predictive input / menu based input functionality should be provided where possible, minimizing user interaction
7.2	Error messages should be standard and not provide too much application information eluding to the reason for the error allowing an attacker to deduce effective attack methods
7.3	Copy and paste must not work for data entry especially when authenticating to the application
7.4	All user input parameters must be validated by the server, and must be validated to accept only values pertinent to the values in the field in accordance with the data dictionary
7.5	Any sensitive content sent to the client machine must not be cached, unless encrypted using approved methods. The application is responsible to set the proper directive to cause the client to not cache the sensitive data
7.6	Sensitive information must not be presented to unauthenticated users
7.7	Sensitive information must not be stored in a persistent cookie, or other location on the client computer that does not have enforceable access control mechanisms.
7.8	Highly confidential data must be stored encrypted
7.9	Confidential data that is stored outside the systems that comprise the application must be encrypted by a firm approved method, such as PGP. This includes file shares, ftp servers, and e-mail
7.1	Functions should not be allowed execute on both encrypted and non-encrypted connections. If functions are required to exist on both encrypted and non-encrypted connections, then the user sessions must not be allowed to span both connections
7.11	Sensitive information must not be stored in hidden fields if the application is web-based

7.12	If data is supplied to the application from an authoritative source, the application must not allow users to modify this data
7.13	The application must not use a credential repository of a trust level less than what is required by the application's data
7.14	User credentials in one repository must not be synchronized with any other repositories unless their trust levels are equal
7.15	If an application uses more than one method or credential store for authentication, all methods and stores used must be at the same trust level
7.16	Web based interfaces should use a secure method to transmit data e.g. Using the HTTP POST method instead of the less secure GET method
8	**Cryptographic Key Management**
8.1	Cryptographic functions must be selected from an approved list. Any cryptographic functions used that are not previously approved require an exception
	Recommended algorithms (with minimum bit lengths), in order of preference, are:
	a) Hashing: SHA -512, SHA -256, RIPEMD160.
	b) Symmetric: AES256, AES192, AES128, 3 -DES (168 bits), Blowfish(minimum 128 bits), Twofish (minimum 128 bits), IDEA (128 bits),and RC4 (128 its).
	c) Public key: RSA(minimum 2048 bits) and DSA(minimum 2048 bits), ElGamal (minimum 2048 bits)
8.2	Any use of hashing must be salted. Values used for salting must be protected
8.3	Encryption keys must be protected during transit and while stored in file system
8.4	Encryption keys must not be disclosed to anyone who does not need access to them
8.5	If using public key cryptography, private keys must be protected by a pass-phrase
8.6	Pass-phrases protecting private keys or used as a share d secret with a symmetric key algorithm must be a minimum of 14 characters in length, and contain at least one upper case letter, one lower case letter, and one number
8.7	A key used to decrypt data must not be stored in the same location as data encrypted with the key
8.8	Site certificates must be current and issued by a well-known certificate authority
9	**Documentation**
9.1	A user manual should be developed as part of the application system/module/component documentation
9.2	A technical manual should be developed as part of the application system/module/component documentation

9.3	An online help facility should be present wherever possible and form part of the application system/module/component documentation
9.4	Signed user requirements/specifications document should be present as it forms the basis for the development of a new application or modification of an existing system
9.5	A Data dictionary should be developed as part of the application system/module/component documentation
9.6	A design blue print with data flow or flow chart diagrams should be present as part of the application system/module/component documentation
10	**Other Considerations**
10.1	A facility should exist to allow rolling-back of transactions/actions under special circumstances clearly documented in the user-specifications. There must be audit trail on the roll-back facility
10.2	Applications should be configurable to securely send audit data/Logs to a centralized data store that is external to the Application Server
10.3	Applications should reliably verify a user's identity using defined multi factor authentication techniques, and capable of secure communication with an external KRA E-directory service for centralized management of authorization and authentication of users to access functionality using security groups defined within the directory service
10.4	Applications should support service monitoring by logging all information that is required for effective monitoring of services based on defined service monitoring parameters
10.5	Applications should have a provision for incorporation of biometrics and related biometric solutions. The next generation of application security would be dependent on biometric identification, authorization and authentication of application users.
10.6	Security for People with Disabilities. Design of Applications should have considerations for people living with disabilities. Varied disabilities calls for design of elaborate mechanisms to enable these group of people to amicably, adequately and elaborately interact with applications. For instance, braille enhanced applications would aid the blind in interacting and using the applications in their endeavours.
10.7	The application should incorporate certified and legitimate digital certificates, which are used to verify that a particular public key (online identity). A PKI is a technical infrastructure that comprises of a Root Certification Authority (RCA) and a Certification Authority (CA), referred to as an Electronic Certification Service Provider (E-CSP) in Kenya's legal and regulatory framework. The generation and usage of the PKIs on an application should be provisioned by the National Public Key Infrastructure for global trust and recognition.

10.8	Personal Identification data(Information) is to be kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and. Personal data shall not be transferred or shared outside the application unless there is proof of adequate data protection safeguards or consent from the data subject. The guidelines for this subject matter are provided by the Kenya Cyber Security Act on Personal Identifiable Information (PII).Ensure the rules of data integrity, confidentiality and availability are adequately adhered to.