Request for Proposal [RFP] for Security Technology Systems.

Copperleaf Country Estate [Copperleaf]

Document Control

Document Information

	Information
Document ID	*D2/2021 – Security Technology*
Document Owner	*Copperleaf Country Estate*
Issue Date	*12/04/2021*
Last Saved Date	*15/04/2021*
File Name	*Copperleaf RFP Security Technology Systems*

Document History

Version	Issue Date	Changes
[1.0]	*21/03/2021*	*New RFP Draft*
[2.0]	*12/04/2021*	*Final for Release*

Table of Contents

1 Introduction

The Board of Directors of Copperleaf have approved the review of the security technical systems at Copperleaf Country Estate.

1.1 Purpose

The purpose of this document is to inform potential suppliers of the detailed information required to enable the **Security Tender Evaluation Committee [STEC]** of Copperleaf to select a preferred supplier who will fulfill the procurement needs of their project.

This information should be submitted in the form of a proposal.

1.2 Acknowledgement

Please acknowledge that you have received this request for proposal by sending a **formal written letter of receipt on a company letterhead via email** to the Security Manager of Copperleaf Country Estate.

Mr. Lance Camphor (Security Manager)
Copperleaf Country Estate
Ernie Els Boulevard
Off West Street
Mnandi
CENTURION
0046

lance@copper-leaf.co.za

If you do not formally acknowledge the receipt of this document within five (5) working days of receiving it, Copperleaf Country Estate will not be able to formally review any subsequent proposal.

1.3 Request for Proposal Process

The **[RFP**] process will be undertaken as follows.

This **[RFP]** will be released to a shortlist of potential suppliers on 24 March 2021.

Suppliers should acknowledge receipt of the [RFP] documentation and **prepare a formal supplier proposal** that will be sent to the General Manager and Security Committee Director of Copper Leaf Country Estate.

The **Security Tender Evaluation Committee [STEC]** will propose a preferred supplier to the **Copperleaf Country Estate Board [BOARD**]. The [BOARD] will approve or reject the supplier services with a resolution of a [BOARD] meeting.

Hereafter, a formal contract will be negotiated with the preferred supplier, and, if endorsed, the supplier will begin with the security service. The following timeframes will be observed during this process:

The Supplier Schedule is available on the Copperleaf Country Estate Website

Release [RFP] documentation
Closure date for receipt acknowledgements
Technical Assessment and site visit by suppliers
Closure date for supplier proposals
Review of supplier proposals complete [BAFO]
Approval and Resolution by the [BOARD]
Preferred supplier notified
Unsuccessful suppliers notified
Draft supplier contract formed
Supplier contract signed
Supplier contract initiated
Supplier Project Schedule agreed and approved
Project Commissioning and Acceptance

1.4 Rules

The supplier response should be accurate at the time of print and remain valid for the remainder of the tender process (as per the above timeframes).

Suppliers may work together to formulate one joint response. However, the full details of each supplier should be included in the supplier proposal.

The supplier should keep all the proposal information confidential as indicated in the entire [RFP]

Formal supplier proposals must be submitted in the form of a printed document. Five (5) copies must be submitted by hand. A further copy (one only) must be captured on a memory device and submitted by hand.

The print documents as well as the memory device must be sealed in envelopes and marked with the [RFP] number and name indicated in this document under the section *document information.*

The sealed print copies as well as the memory device must be handed to the General Managers Secretary at the administration offices at the Golf Club on or before the closing date. The delivery address is the *domicilium citandi et executandi* mentioned in item 1.2 above. In addition, supplier is required to complete the proposals register when delivering the documents and memory device. Proposal will only be accepted during office hours from 08h00 to 15h00, Mondays to Thursdays. No late submissions will be accepted.

1.5 Questions

The supplier may have questions pertaining to the proposal process or matters appropriate to the **[RFP]** information. **No questions will be entertained after the closure of the submission of proposals date. No questions will be permitted via telephone. All the questions raised will be shared with all the suppliers.**

These questions should be directed via email to:

Copperleaf Country Estate
Ernie Els Boulevard
Off West Street
Mnandi
CENTURION
0046

lance@copper-leaf.co.za

1.6 Risks

Supplier must express any risks anticipated during the acknowledgement or questions phases of this [RFP] process.

1.7 Compliance Checklist

Copperleaf has included a supplier compliance checklist. Supplier must complete every section of this checklist and submit it with the proposal.

2 Supplier Company Information

COPPERLEAF DATA PROTECTION AND PRIVICY POLICY APPLIES.
SUPPLIER INFORMATION TO ACCOMPANY PROPOSAL

Title (Prof / Dr / Mr / Mrs / Ms) and Surname	
Sole Proprietor Identity Number	
Registered Name of Business	
Trading As	
Business Registration number	
SARS Tax number	
VAT Registration number	
Physical address of business:	
Building / Complex name	
Street name and number	
Suburb	
City	
Postal code	
Country	
Postal address of business:	
Postnet address	
P.O. Box / Private Bag	
City/Town	
Code	Code: Number:
Contact Details:	
Business telephone number	
Order e-mail address	
Supplier e-mail address	
Remittance e-mail address	
Business Contact person / Sales Rep	
Name	
Telephone number	
E-maill address	
AFFIRMATION OF INTEREST Does any of the directors / owners / partners have any connection or vested interest in Copperleaf or any of its operations or if any has been or are currently employed with Copperleaf or any of its operations? ☐Y ☐N	

HDSA SUPPLIER RATING CRITERIA FOR SUPPLY AND TENDER EVALUATION

Criteria	Yes / No	%	
Black Ownership			
Black Women Ownership			
Employment of Black Disabled			
Procurement from Black / HDSA Suppliers			
Procurement - % Local goods			
Procurement - % Imported goods			
Other HDSA Initiatives			
What is your BEE Level?			
If Non-Compliant, please Elaborate:			

I hereby authorize Copperleaf to perform a BEE and Credit Check with third party service providers for the purpose of this application

☐Y ☐N

TYPE OF BUSINESS:

An Agent ☐ Manufacturer ☐ Distributor ☐ Consultant ☐ Contractor ☐

Type of goods and/or services rendered:

_____

Commercial

Name three commercial references/referees of previous projects and provide their name(s) and telephone number(s):

COMPANY	CONTACT PERSON	TELEPHONE NUMBER

Financial

Has any party to this application ever been declared insolvent, placed in liquidation whether provisional or final or reached a compromise with creditors or have been subject to 'business rescue', is financially distressed or subject to supervision as defined in Chapter 6 of the Companies Act?

☐Y ☐N

Criminal Record

Has any party to this application had any pending or criminal convictions involving dishonesty or paid and admission of guilt other than speeding or parking offences?
☐Y ☐N

Standard

1. Are you working to National or International Standards?
   ☐Y ☐N

_____

Quality

1. Does your business operate a Quality Management System covering the Product/service applying for?
   ☐Y ☐N

2. Has your Quality Management System been assessed and certified by any National/International recognized accredited body?
   ☐Y ☐N

Safety

1. Does your business have a Occupational Health and Safety Policy Complying with the Occupational Health and Safety Act (OHSA)?
   ☐Y ☐N

2. Does your business comply with Compensation for Occupational Injuries and Diseases Act (COIDA)?
   ☐Y ☐N

Human Resources

1. How many employees are employed? ☐
2. Are your workers covered by medical aid?
   ☐Y ☐N
3. Do you provide Pension or Provident Fund?
   ☐Y ☐N
4. Do you provide Death benefit?
   ☐Y ☐N
5. Is your company registered for COIDA?
   ☐Y ☐N

SUPPORTING DOCUMENTS REQUIRED

Please attach copies of the following documents which should be **signed and certified by a Commissioner of Oath:**

Company Registration Document.
Company Registration Document with the Private Security Industry Regulatory Authority.
Proof of Membership with SAIDSA
List of Directors / Partners / Sole Propriety, ID number and a copy of the ID document.
Shareholders Agreements / Certificates for companies claiming Black Empowerment.
Financial statements / letter from your auditors indicating maximum size or business capability.
VAT 103 certificate where applicable.
SARS Tax Clearance Certificate.
BEE Certificate
Letter of Good Standing from COIDA (workman's comp) or RMA
Letter from the Bank confirming your company's banking details.
Company Letterhead.

If there are any changes to the information supplied on this form, please inform Copperleaf within 28 days. Outdated information could potentially lead to your company not being invited for proposals or not receive payment timeously.

2.1 Offering

The supplier should include a company profile with the proposal.

The following information should also be included.

Products offered, including goods and services,
Locations currently served,
Market segments within which the company operates,
Market share captured, and
Competitors

2.2 Experience

The following information should also be included by the supplier:

Number of years selling products within each market segment,
Average number of years each staff member has been with the company,
Level of knowledge of industry,
Level of knowledge of products offered, and
Level of expertise in products offered.

REQUIREMENTS STATEMENT

PART A – COPPERLEAF CHARACTERISATION

3 REQUIREMENTS STATEMENT

3.1 PART A – COPPERLEAF CHARACTERISATION

Part A of the operational requirement provides the supplier with an understanding of the problem the estate owners are addressing.

3.1.1 Site Plan

A site plan is attached to this [RFP]. The plan is marked with the general location of the current security technology. The supplier should review the technology location to determine what would be required to mitigate the threats mentioned in **section 3.1.2.**

3.1.2 Problem Statement

Copperleaf has undertaken a security risk analysis. The data from the analysis indicates that the estate may be the target of the following serious crimes in the future. Ongoing security risk analysis will inform future developments and trends.

Robbery of Motor Vehicles (Carjacking) (RMV),
Sex Offences (SOF),
Theft of Motor Vehicles (TMV),
Robbery with Aggravated Circumstances (AGC),
Theft out of Motor vehicles (OMV),
Burglary (Housebreaking) (BRS),
Robbery Common (RBC),
Narcotic Offences (NAR), and
Other “lesser” crimes not listed here such as petty theft et cetera.

Figure 1 is the risk matrix that indicates the intersection of **likelihood and impact of these potential serious crimes.**

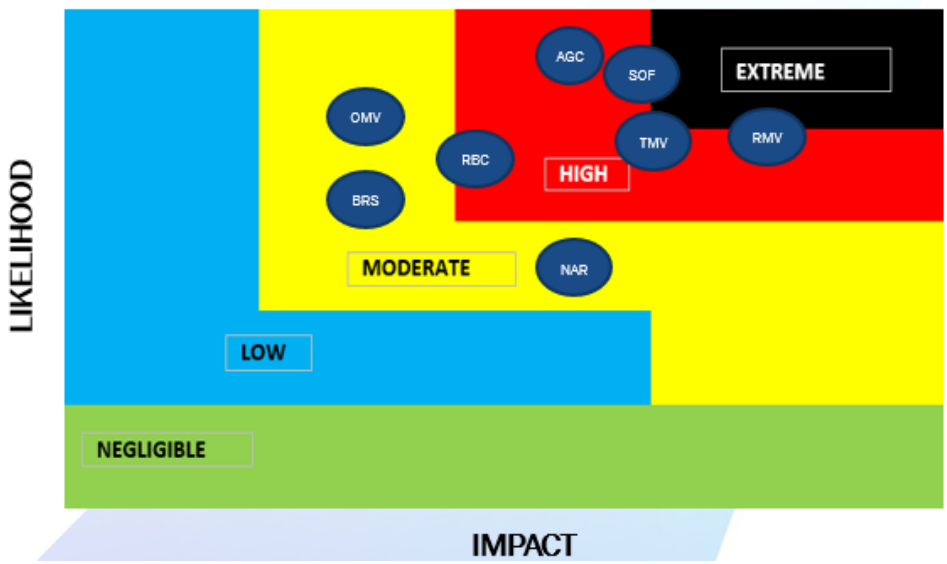


Figure 1: Risk Matrix of probable crime.

There are other security issues which exacerbate the potential for other crimes or incidents in general.

These include but are not limited to:

Large pedestrian flows,
High volume of vehicle movement,
Trespass,
Loitering,
Scouting to plan serious crime,
Unauthorised entry to commit other crime,
Hostile vehicle threats on access and egress.

3.1.3 Security Principles

The success of the security measures which the supplier proposes will be best measured with the following statements.

Deterrence. That is unauthorised persons are prevented from entry.
Deny access to unauthorised persons or vehicles. Especially hostile vehicle threats.
Delay the advance of an adversary.
Detect any unauthorised or suspicious activity in the estate and on the perimeter.
Defend inwards as well as outwards.
Divided into manageable zones.
Defeat the adversary.
Deflect an adversary onto a weaker target.

REQUIREMENTS STATEMENT

PART B – PHYSICAL PROTECTION SYSTEM DESIGN [PPS]

3.2 PART B – PHYSICAL PROTECTION SYSTEM DESIGN [PPS]

Part B addresses those aspects of the technical systems which will form part of the physical protection system **[PPS]** of Copperleaf. The [PPS] integrates people, procedures, equipment and **technology** for the protection of assets or other malevolent human attacks.

The supplier is required to demonstrate that the technology which is proposed is capable to **detect, delay and respond** to actions of incidents and crime.

Detection is the discovery of an adversary action. It includes sensing of covert and overt actions. The measure of effectiveness for the detection function are the probability of sensing adversary action and the time required for reporting and assessing the alarm.

Delay is the second function of a [PPS]. It is the slowing down of adversary progress. Delay can be accomplished by personnel, barriers, locks, activated delays and **technology.**

Response actions are taken by the security response force to prevent adversary success.

3.2.1 Technical Assessment

Location

The supplier should conduct an **on - site technical assessment and attend the compulsory briefing** to determine the appropriate fit for purpose technology.

The security management of Copperleaf will facilitate the assessment by prior appointment and **in the time frame of the project schedule.**

The supplier is required to divide the site (Copperleaf Estate) into specific zones or locations.

A location may either be an area where a particular threat exists, or it may be a strategic location away from the threat, but where monitoring would be appropriate because high quality images or information of the offender could be obtained, such as a pinch point or turnstile for access and egress. Consider whether there is a need to monitor throughout the site in order to track individuals and be aware of the location of any blind spots.

It is also possible that two or more separate activities require monitoring in a single area such as a car park (golf club), offices (Home - Owners Association offices and stores) or an entrance. Treat each scenario separately when preparing your proposal.

Modus Operandi

The supplier should ensure that the potential threats mentioned in **Part A** of this section are able to be monitored, detected and deflected.

Examples include, but are not limited to:

The action to climb over, dig through or dig under the perimeter wall,

The action to commit robbery by driving a hostile vehicle or vehicles down the Ernie Else Boulevard,

Actions of threats at the access / egress points to the estate.

Purpose of the observation

The supplier should assess and advise which of the ***five levels of detail*** described in **section 3.2.2** is most appropriate to the surveillance requirement.

That is to:

Monitor a large area,
Detect individuals approaching the estate,
Observe the actions of a group of adversaries,
Recognise known individuals at an entrance, and
Obtain images that would enable the estate security (or the police) to identify an unfamiliar individual.

A typical fixed camera can be specified to cover a narrow field of view with a high level of detail (for recognition / identification purposes), or a wide field of view at a lower level of detail (for monitoring / detection), but generally not both. To this end it is important to consider carefully which of these requirements is the more appropriate for each location.

3.2.2 Closed Circuit Television [CCTV]

Most camera systems are designed to observe human activity. The application, however, can range from crowd control / public safety (where the movement of large numbers of people needs to be monitored over a wide area) to access control (where close-up, high quality imagery is required to enable individuals to be identified). The choice of [CCTV] camera will depend on the nature of the activity to be observed.

To simplify the situation and to provide guidance to a system supplier, five. general observation categories have been defined, which are based on the relative size that a person appears on a [CCTV] screen.

As part of the technical assessment by a supplier, they should, in conjunction with Copperleaf, determine which of these four categories best reflects the type of activity being observed.
The supplier and their [CCTV] installer will then fit a suitable camera to meet the requirement.

Monitor and Control: A figure occupies at least 5% of the screen height and the scene portrayed is not unduly cluttered. From this level of detail an observer should be able to monitor the number, direction and speed of movement of people across a wide area, providing their presence is known to him/her.

Detect: The figure now occupies at least 10% of the available screen height. After an alert an observer would be able to search the display screens and ascertain with a high degree of certainty whether or not a person is present.

Observe: A figure should occupy between 25% and 30% of the screen height. At this scale, some characteristic details of the individual, such as distinctive clothing, can be seen, whilst the view remains sufficiently wide to allow some activity surrounding an incident to be monitored.

Recognise: When the figure occupies at least 50% of screen height viewers can say with a high degree of certainty whether or not an individual shown is the same as someone they have seen before.

Identify: With the figure now occupying at least 100% of the screen height, picture quality and detail should be sufficient to enable the identity of an individual to be established beyond reasonable doubt.

3.2.3 System Requirements

Alert Functions

As part of the operational assessment the supplier should advise what type of activity should trigger an alert, and then what form that alert should take.

The following requires assessment and recommendation.

a simple audible alarm such as a beep,

visual alarms such as a flashing light that pinpoints the location of the event on a plan of the facility on a screen in front of the operator,

a text message or an image sent to a key holder or security manager,

an emergency relay sent to the alarm monitoring company,

a record of the event data,

display the view from the camera on a monitor screen in front of the operator (It may be advisable for some monitor screens in the control room to remain blank under normal conditions, and to be activated only when an event is detected.),

create a record of the event in an audit log,

to prove that the system is functioning correctly and that nothing of interest occurred during the times it was not recording.

Display

Live monitoring will be performed in the Copperleaf Security Control Room on a twenty - four (24) hour basis, every day and all year.

To this end the supplier should advise on the following aspects:

The number of screens required based on the number of cameras,

The balance between number of operators and how many displays they can effectively monitor at any one time,

Some camera views may require constant monitoring and will thus need a dedicated screen; others may not in which case a single screen could be used to cycle between several cameras.

Separate displays (or a separate viewing area) may be required for reviewing recorded video.

The type of display is a choice between traditional CRT screens and more modern LCD, or plasma displays.

Automatic Number Plate Recognition [ANPR]

The supplier should ensure that automatic number plate recognition forms part of the integrated system.

[ANPR] uses a camera connected to a system with optical character recognition to identify the numbers and letters on a number plate. This number is recognised and compared against a list of authorised vehicles stored in a database.

To improve the reliability of an **[ANPR]** system, the camera should be located where vehicles are lane controlled or constrained by a narrow width, where the vehicles are viewed head on and as close as possible.

Recording

The supplier should ensure that a **retention time of sixty (60) days** is maintained for all camera footage until it is overwritten.

An additional facility of protecting sequences of particular interest at access points to the estate should prevent them from being overwritten.

Digital video recorders will be required. They save images which are compressed so that more data can be saved on the hard drives. This compression will almost invariably reduce the quality of the video.

Recorders are vital to inspect the quality of the recorded images as well as the live view as there could be a substantial difference between the two.

Adjusting the recorder settings to increase the retention time will result in a reduction in the stored image quality (i.e. “Best Storage” settings give you the lowest quality recorded video).

The supplier should advise on the frame rates and recording time to ensure the integrity of quality images.

Additional metadata (text information) should be recorded alongside the video images. A key requirement is to include the time and date information, firstly to add evidential weight to the pictures, and secondly to allow the user to search through the recordings and retrieve the relevant video efficiently.

There is a requirement to record the camera location and number.

Include a mechanism for ensuring that the time and date information remains accurate (for example during the change from GMT and does not slowly drift from the true value. This mechanism can either be technical (such as the inclusion of a clock source automatically linked to the NPL time signal) or procedural (instruction to the operator to check and update the clock regularly).

The supplier should propose a system to protect the recording system against the possibility of hard drive failure.

This is usually achieved by specifying a RAID recording system (Redundant Array of Independent Discs). There are several RAID standards, but they commonly involve splitting / duplicating the data across more than one hard drive.

The RAID system should be fail - safe.

Other aspects to consider with recording include:

Compression,
Effect of compression on quality

Cascaded compression,
Frame Rates,
Storage capacity,

Export / Archiving

The supplier should ensure that the CCTV recorders provide a means of creating a permanent record of an incident, which can then be provided as evidence for any subsequent investigation.

The CCTV system therefore needs to be provided with a suitable export facility. In most cases a DVD writer will suffice for exporting single images and short video clips under about ten minutes in length.

For exporting longer video clips and for large scale archiving, the system should provide one of the following:

the ability to export video to an external ‘plug and play’ hard drive via a USB or Firewire connection,

Network port, or

Removable hard drive.

3.2.4 Technical Guidance

Lighting

The supplier should cooperate with the management of Copperleaf and provide guidance with the positioning of lights for the CCTV. The correct light levels as well as scene contrast will help to ensure that the system performs to the best of its ability.

Light Level

It is important to maintain a suitable light level over the scene being monitored. The minimum light level required will depend on the type of activity being monitored.

Most cameras can operate at surprisingly low levels, well below the 3-lux figure generally considered as the minimum for security purposes. A lighting schedule will have to be agreed with Copperleaf Management.

As with our own vision, systems tend to be weaker at discerning colours and detail at low light levels and this gets worse as the light level drops. Picture quality should not be compromised as a consequence of this.

Scene Contrast

Keeping even levels of light across a scene ensures good contrast.

Combining extreme levels leads to too much contrast resulting in a poor image.

There should not be a poor ratio of minimum to maximum illumination within an artificially lit scene.

Field of View (FoV)

Also referred to as the angle of view or angle of coverage. The [FoV] is the amount of a given scene captured by a camera.

To ensure an effective field of view the supplier should ensure that the camera is positioned to focus on a specific risk. These are highlighted in **Part A** of this [RFP].

Having determined the area of interest, the activity to be monitored, the observation criteria and target speed as part of the capture process, it should now be possible to estimate the most suitable [FoV]. When determining the [FoV] required of a camera avoid problem areas such as shadows and blind spots, and care should also be taken not to record areas outside the remit of the installation.

The CCTV for the perimeter is expressed in the section marked Perimeter Intrusion Detection Systems [PIDS]. Save to say that the [FoV] should overlap and ensure cross protection of other cameras to remove any unprotected zones.

Features

The supplier should indicate if the CCTV is capable of the following features and advise where these should apply. This is done after the technical assessment by the supplier is complete.

On board image processing,
Automatic gain control,
White balance and colour, and
Image resolution at the camera,

Camera and infrastructure placement

The supplier should consider the following points for camera and infrastructure positions:

Create the required field of view. Camera placement should be based on achieving an optimum view. The choice of location should not be dictated by ease of installation. The installation should have a risk focus.

Consider the effects of daily and seasonal variations in light especially low sun and mist due to weather changes.

Consider the changes in foliage growth between winter and summer.

Consider protection from damage and the environment such as vandalism or driving rain.

Be aware of temporary or new permanent structures such as signs or other buildings blocking the [FoV].

Remember the need to perform maintenance such as cleaning or repairs.

Consider how power will be supplied to the camera and data transmitted from it.

Ensure that the camera is fixed firmly and does not wobble in the breeze or through mechanical vibration. Stability may be a problem if the camera is fixed to a tall pole in an exposed location.

Where suspect identification is the main priority, place the camera at head height. Ceiling mounted cameras may not be able to provide a full view of the suspect's face.

When using the identify criteria it is recommended that clear space is left above the head in order to allow for variations in person height and discrepancies in recording systems.

Transmission

The technology used for transmitting the video signal from one location to another is a key component of any CCTV system. There is an increasing array of options available, moving away from the traditional standard analogue coaxial cable solution, and so more thought now needs to be given to the choice of transmission method.

The most significant advance in recent years has been the development of IP based transmission. This is an approach for transmitting any digitised data in a robust and manageable way over a variety of link types. Its use in the CCTV field is growing, and often results in new approaches to solving problems.

As with any system design it is important that the supplier understands the implications of choosing one method over another. Both the physical and financial constraints of the intended CCTV system need to be considered.
The supplier should advise on these options with the comparative pricing.

The optional items that need to be explained and included are:

Video signal type,
Wired transmission,

Wireless transmission, and
Display type.

Image quality

The supplier should ensure that the CCTV image quality is of a high standard. To This end the following features should be considered:

Clarity – Is the picture sharp enough, and is there any lens distortion? Ensure that the lens or lens / camera combination is of sufficient quality for the task in hand.

Detail – Is there enough to identify objects? Check that image quality is not compromised by trying to achieve a large [FoV] at the cost of image detail, and that lighting levels permit a useable depth of focus. If necessary, break the scene into smaller sections.

Colour – Is it natural? Is it necessary? If accurate colour reproduction is important then ensure the lighting is of sufficient quality and quantity to allow the cameras to achieve this.

Artefacts – Are there elements in the image that should not be there? And if so, are they obtrusive? If this is the case then depending on the artefact, either the amount of compression that needs to be reduced or the camera/lighting placement needs to be addressed.

Redundancy

The supplier should ensure that all the technology proposed has a backup system which is maintained to ensure reliability and availability.

3.2.5 System Validation

The supplier should undertake to validate the system at intervals determined by Copperleaf.

The measures which may be assessed during the project process would include:

Safety and Health,
Continuous system design compliance to address risk,

Before System Commissioning to view the live product, the recorded product and test target evaluation as well as a system audit.

3.2.6 Perimeter Intrusion Detection Systems [P.I.D.S.]

Performance Characteristics

Copperleaf is equipped with a wall and palisades around the perimeter of the property. A clear zone (road) around the property seems impossible due to a number of factors. To this end the property should be well protected with [PIDS].

The supplier should ensure that any proposed system should have a high probability of target detection with an equally high confidence level.

Equally, the nuisance alarm rate should be kept to a minimum.
The supplier should agree with Copperleaf what an acceptable false alarm rate will be.

All sensors can be defeated.
To prevent vulnerability to defeat the supplier should consider the following measures:

the cost of design for both the installations and the life cycle,
creation of additional vulnerabilities,
safety issues,
increases in manpower,
increased training requirements,
design life,
system effectiveness against the specified threats,
possibility just accepting the risk associated with leaving a vulnerability in the design.

Sensor Classification

The supplier will indicate what type of sensors are proposed under the following categories:

Passive or active,
Covert or Visible,
Line of sight,
Terrain following,
Volumetric,
Line detection, and
Application.

Sensor Technology

The supplier should propose what [PIDS] technology is the best option to address the threats mentioned under the following types:

Buried Line Sensors,
Pressure or Seismic,
Magnetic Field,
Ported Coaxial,
Fibre Optic Cables,
Fence Associated Sensors (Including an Electric Fence),
Electric Field or Capacitance,
Freestanding Sensors,
Active Infrared,
Passive Infrared,
Bistatic Microwave,
Video Motion Detection,
Passive Scanning Thermal Imagers,
Active Scanning Thermal Imagers,
Wireless Sensor Networks,
Red Fore / Blue Force Tracking,

Continuous Line of Detection

The design goal is to have a uniform detection around the entire length of the perimeter. The perimeter is divided into sectors to aid in assessment and response.

Protection in Depth

The concept of protection in depth means the use of multiple lines of detection.
To this end the supplier should propose three (3) sensor lines. These may be a buried line sensor (overt), CCTV active scanning thermal image (covert and overt) and Electric Fence Sensors (covert).

Tamper Protection

The hardware and system design should incorporate features that prevent defeat by tampering. The system should be tamper resistant and tamper indicating.

Self - Test

To verify normal operation of the perimeter sensor system, its ability to detect should be regularly tested. Albeit that it will be tested manually (stress tested) by security management of Copperleaf it should have the capability for remote testing of trigger signals.

Pattern Recognition

The system should be able to receive signals from sensors and analyse the signal pattern, looking for patterns that are particularly characteristic of an intruder.

The system should be able to use artificial intelligence software to learn intruder signal patterns and avoid nuisance alarms.

Environmental Conditions

The supplier should take into account the environmental conditions that can effect the [PIDS] and take preventative measures.

These are, but not limited to:

Topography,
Vegetation,
Wildlife,
Background Noise,
Climate and Weather,
Soil and Pavement,
Lightning Protection

Integration with a Video Assessment System

The perimeter security systems should be integrated into the CCTV system to perform alarm assessment.

The video assessment should be automatically tied to sensor activation to reduce the time to determine the alarm source.

3.2.7 Internal Intruder Detection Systems (IDS)

Performance Characteristics

Copperleaf has critical assets in the form of buildings and outdoor infrastructure.
Examples are the Home - Owners Offices, Administration Offices, Golf Club and Sewerage Works.

Copperleaf will provide a list of areas that should be the subject of internal intruder (alarm) monitoring. These areas should be protected.

The supplier should ensure that any proposed system should have a high probability of target detection with an equally high confidence level.

Equally, the nuisance alarm rate should be kept to a minimum.
The supplier should agree with Copperleaf what an acceptable false alarm rate will be.

All sensors can be defeated.
To prevent vulnerability to defeat the supplier should consider the following measures:

the cost of design for both the installations and the life cycle,
creation of additional vulnerabilities,
safety issues,
increases in manpower,
increased training requirements,
design life,
system effectiveness against the specified threats,
possibility just accepting the risk associated with leaving a vulnerability in the design.

Sensor Classification

The supplier will indicate what type of sensors are proposed under the following categories:

Passive or active,
Covert or Visible,
Line of sight,
Terrain following,
Volumetric,
Line detection, and
Application.

Sensor Technology

The supplier should propose what Passive Infrared [PIR] technology is fit for purpose to detect internal intrusion to buildings.

The following should be included:

Well defined detection zones,
No interference between multiple devices, and
Moderate cost,

Tamper Protection

The hardware and system design should incorporate features that prevent defeat by tampering. The system should be tamper resistant and tamper indicating.

Self - Test

To verify normal operation of the perimeter sensor system, its ability to detect should be regularly tested. Albeit that it will be tested manually (stress tested) by security

management of Copperleaf it should have the capability for remote testing of trigger signals.

Pattern Recognition

The system should be able to receive signals from sensors and analyse the signal pattern, looking for patterns that are particularly characteristic of an intruder.

The system should be able to use artificial intelligence software to learn intruder signal patterns and avoid nuisance alarms.

Integration with Video Assessment System

The internal intruder detection systems should be integrated into the CCTV system to perform alarm assessment.

The video assessment should be automatically tied to sensor activation to reduce the time to determine the alarm source.

3.2.8 Access / Egress Control (AEC)

Performance Characteristics

Copperleaf Estate has three primary access and egress facilities. The supplier should review the access and egress [AEC] automated access management system with the objective to:

Prevent unauthorised entry,

Facilitate authorised entry,

Prevent the introduction of prohibited items,

Prevent the unauthorised removal of property,

Monitor and control egress,

Provide an account of who is on the estate at any given time,

Provide information to security management,

Prevent unauthorised observation of sensitive processes/operations, or compromise of sensitive information,

Protect the home - owners, tenants, visitors and their property.

Prevent hostile attack or abuse, (armed robbery or other serious crime),

Provide an audit trail of access/egress transactions.

The easier it is to access the estate, the more likely the system will grant access to unauthorised persons.

Automated Access Management [ACMS]

The supplier should ensure that the access and egress [AEC] automated access management system [ACMS] is capable of the following features.

It can work well with existing gate, turnstile and door hardware and locking systems,

It is competitively priced and delivers good value,

It is adaptable to re-scaling and integration with other physical protection elements,

It has the capability to deliver added return on investment through additional functionality, such as time and attendance.

It takes account of the accessibility needs of less able people and any relevant associated legislation.

Biometrics

Copperleaf Estate has two primary access and egress routes at each access control facility. That is vehicle and people routes. The supplier should review the access and egress [AEC] automated access management system [ACMS] for each route. That is both access and egress.

Copperleaf Estate uses biometric technology for both access and egress management.

Biometric data is something that you are.

Biometric Verification (Also known as “One to One” (1:1) technology) is where the user’s biometric sample is compared to a single template stored by the biometric system. The system then verifies that the biometric feature matches the information stored against the user already identified.

The supplier should propose options to replace the current biometric [ACMS] by any of the following:

Fingerprint identification,
Facial Recognition,
Iris or Retina Recognition,
Hand Geometry identification,
Vein Recognition, and
Voice Recognition.

Authorisation Profiles

The supplier should ensure that all persons enrolled into the [ACMS] should be allocated an authorisation profile. This may be specific to the individual or to a group of people. The authorisation profile defines the ability of the biometrics.

Authorisation profiles should include the following:

Access level.

Zone.

Turnstile, Gate or Door.

Authorised time schedules,
Previous events,

Alarm condition.

Anti – Pass back Function – People.

The [ACMS] should include two types of anti – pass back features.

Hard anti-pass back disallows a second access to an area if a valid exit has not previously been registered and generates an alarm,

Soft anti-pass back does allow a second access to an area if a valid exit has not previously been registered but generates an alarm. Anti-pass back rules are generally reset after a pre-set period after valid entry, at a fixed time each day, on exit from site or manually as an over-ride.

Anti – Tailgate Feature - Vehicles

The [ACMS] should include two types of anti – tailgate features.

Hard anti-tailgate employs physical means such as bollards to restrict movement.

Soft anti-tailgate does not prevent the unauthorised vehicle but uses detection methods to generate an alarm, for example an infrared beam.

Integration of the [ACMS]

The supplier should ensure that the automated access management system [ACMS] is capable of integration with other [PPS] systems.

Vehicle Barriers

Hostile vehicles can drive or crash through most gates, booms or poor access / egress points.

The supplier should incorporate vehicle barriers that should be installed inside the detection and assessment zone to ensure valid delay.

The following should be considered for the vehicle barriers:

The threat that the barrier system is intended to stop,

The weight of vehicles,
Impact velocity,
The ability to reduce speed before impact to the barrier,
The access control offices should be protected from physical force,
Other physical characteristics, and
The barriers should be connected and operated via the [ACMS].

Radio Frequency Identification Tags (RFID)

The supplier should ensure that the [ACMS] has the capability for incorporation of (RFID) for key assets as part of red/blue force tracking.

This feature will sound an alarm if any key asset marked with (RFID) enters an egress assessment zone. The egress controls should then lock down the movement and call for assessment.

Magnetometers

The supplier should ensure that magnetometers are incorporated at access and egress facilities for scanning pedestrians.

Options of hand - held as well as walk through units should be provided in the proposal.

Guard Patrol Tracking – Real Time and Recorded

The supplier mut provide options for real time security guard tracking.

The options should be able to be integrated into the system and provide for screen monitoring.

Security Vehicle Tracking – Real Time and Recorded

The supplier mut provide options for real time vehicle tracking.

The options should be able to be integrated into the system and provide for screen monitoring.

REQUIREMENTS STATEMENT

PART C – MANAGEMENT REQUIREMENTS

3.3 PART C – MANAGEMENT REQUIREMENTS

3.3.1 Management Issues

Legal Issues

The supplier should ensure that the capture of data is compliant with the laws of the Republic of South Africa. In particular, the Protection of Personal Information Act 4/2013.

The supplier should comply with the laws of the Republic of South Africa before, during and after the project timeline.

Maintenance

Without ongoing maintenance, the systems will deteriorate.

The supplier should provide a plan for maintenance which includes but is not limited to the following:

Cleaning the equipment (Especially cleaning the camera housings, lenses and gear),

Repairing or replacing faulty equipment (an acceptable turnaround time from report to repair should be specified in [RFP] return,

Fitness for purpose checks (including who performs them, and what activities are undertaken),

Maintaining camera positions and focus,

Upgrading the system (The expected working life of the equipment should be known, and upgrades planned for.)

Equipment warranties.

If cameras are placed in awkward or inaccessible locations, then maintenance could be more difficult. Health and safety regulations may also need to be consulted when carrying out maintenance operations.

Performance

The supplier should demonstrate that every system installed is measured by real time data to report on the following **performance metrics:**

Uptime is a measure of system reliability, expressed as the percentage of time a machine, typically a computer, has been working and available. Uptime is the opposite of downtime. This should be maintained at >95%.

Mean Time to Repair (MTTR) refers to the amount of time required to repair a system and restore it to full functionality. A time schedule for each item should be agreed with the management of Copperleaf.

The **(MTTR)** clock starts ticking when the repairs start and it goes on until operations are restored. This includes **repair time, testing period, and return to the normal operating condition**.

Mean time to failure (MTTF) is a maintenance metric that measures the average amount of time a non-repairable asset operates before it fails. Because MTTF is relevant only for assets and equipment that cannot or should not be repaired, MTTF can also be thought of as the average lifespan of an asset.

Products

The supplier is required to provide a separate product inventory list of every item proposed for this [RFP].

This should include the following as a minimum:

Product name,

Product description,

Product components (if the product is a good)

Product activities (if the product is a service)

Product quantity (i.e., the number of each particular product proposed)

Product purpose (i.e., its use)

Product capabilities

Product quality

Note: This section is a very critical section in the [RFP]. It is important to stress to the suppliers that they should provide detailed information for this section to allow the **[STEC] Team** to gain a full appreciation of the solution that the supplier is offering the project.

Training

The supplier should indicate the following:

Products for which training is necessary,

Proposed method of training (e.g., one-to-one, classroom, train-the-trainer)

Level of training to be given (e.g., beginner, intermediate, or advanced)

Number of trainees to be given training.

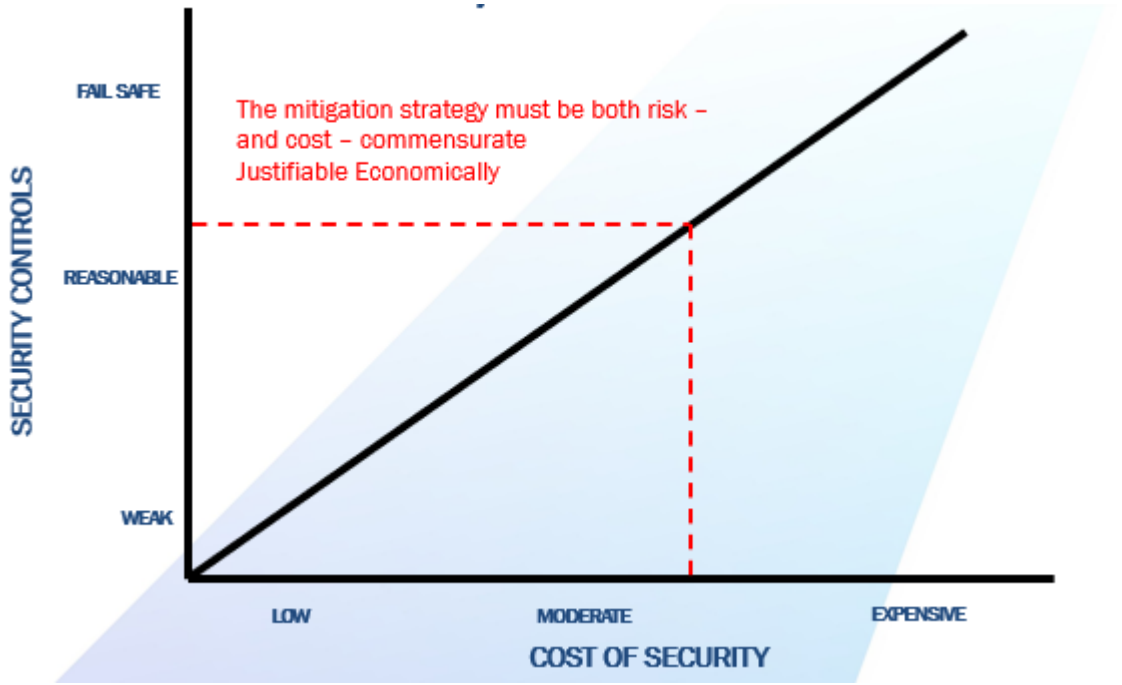
Information

The following information will be required by Copperleaf:

Products for which documentation will be provided,
Actual documents to be generated,
Purpose of each document provided,
Depth of each document provided,
Target audience for each document provided,
Product specifications or marketing brochures,
Website addresses for product listings,
Profiles of staff providing services

ALARP – (Risk) As Low as Reasonably Practical

The supplier needs to take into consideration that the further objective of this [RFP] is to reduce **risk to "as low as reasonably practicable" or ALARP not exceeding excessive cost.**



Quality and Conformance

Where applicable, every installation shall comply with the SANS 10222 standard and the parts applicable that are framed thereunder.

Turn - Key Project

The supplier should manage and deliver all the elements of the project in accordance with the pre - approved agreed project schedule. The project will be regarded as a turn – key project. Implying that upon commissioning all elements and segments of the system will be fully operational to the satisfaction of **Copperleaf [STEC]**

Confidentiality

During this proposal process you may acquire confidential information relating to our business, project, and/or stakeholders.

You agree to keep this information strictly confidential. Even after the project has been completed.

You will not use, or attempt to use, this information for your personal gain or the gain of any other person.

You may disclose confidential information only to the extent that such disclosure is necessary for the submission of a formal supplier proposal.

This agreement does not apply to information that should legally be disclosed or that becomes available to and known by the public.

Guarantees

Supplier must agree with Copperleaf all guarantees of all the equipment installed to ensure mean time to failure is well within the expected life cycle of such equipment.

Quantity Survey

Supplier must agree with Copperleaf the process for quantity survey of all installations and supplies. This cost must be included in the [RFP]

Project Schedule

Supplier must agree with Copperleaf a project schedule of all the installations. That is from the start date to commissioning and acceptance of those agreed items.

Penalties for late completion / commissioning

The commercial agreement will contain provisions for penalties due to late completion of the project.

Note: If the supplier does not agree with the respective clauses, then s/he should explicitly state it within his/her proposal.

STANDARD TERMS AND DEFINITIONS.

Adversary – An individual or group that is motivated and capable of stealing, damaging, or destroying critical assets. They can include insiders, outsiders, or a combination of insiders and outsiders.

Adversary Pathway – The most objective route of least resistance used by an adversary to commit crime.

Action – What is it the adversary may seek to do (loss, denial, destruction, compromise) *Modus Operandi.*

Active Surveillance – All early warning systems that signal intrusion or crime in progress but are monitored by security personnel in real time and who can initiate immediate response.

ACMS – Automated access management system.

Alert – A signal that can not be missed to trigger assessment and reaction to an incident.

ALARP - As Low as Reasonably Practical but not exceeding excessive cost

Asset – People, property and information. People may include employees and customers along with other invited persons such as contractors or guests. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.

ANPR – Automatic Number Plate Recognition.

ACB – Access Control Building.

Capability – The capability of an adversary to obtain, damage, or destroy an asset.

CCTV – Closed Circuit Television

CCTV Detection – Where about 10% of the image occupies the screen.

CCTV Observation - Where about 25% of the image occupies the screen.

CCTV Recognition - Where about 50% of the image occupies the screen.

CCTV Identification - Where about 99% of the image occupies the screen.

Consequence – The extent of loss that can be anticipated from a successful adversarial attack against an asset. The impact of loss may be human, economic, political, environmental, or operational; however, consequences should be stated in financial terms if possible.

Continuity of Operations (COOP) – A concept that seeks to ensure that an organization's essential functions and mission-critical operations can be performed.

Cost-Benefit Analysis [Also ALARP] – An assessment conducted during the countermeasure selection phase of the costs and benefits of each security measure option. Costs typically include the money and time resources required to implement the measure and any ongoing time and money needed to maintain the measure. Benefits are security program improvements derived from planned security measures.

Countermeasures – Security measures that include policies and procedures, physical security equipment and protection systems, and security personnel. The primary purpose of a countermeasure is to mitigate risk through a prevention process that eliminates or neutralizes threats and reduces vulnerabilities. The term *countermeasures* are used interchangeably with security measures.

Crime Analysis – The logical examination of crimes that have penetrated preventative measures, including the frequency of specific crimes, each incident's temporal details (time and day), and the risk posed to a property's inhabitants, as well as the application of revised security standards and preventative measures that, if adhered to and monitored, can be the panacea for a given crime dilemma.

Criticality – The operational impact to the organization's mission due to the loss, damage, or destruction to an asset.

Defeat – A security strategy designed to neutralize adversaries before an asset is lost, damaged, or destroyed. For defeat to occur, the security program to be operating at an optimum level.

Delay – A security strategy designed to slow the progression of adversaries into or out of the facility. Barriers are an example of a delay measure.

Detection – A security strategy designed to assess the threat and to alert security personnel of an adversary's presence. Cameras and sensors are examples of detection measures.

Deterrence – A security strategy designed to discourage adversaries by increasing the risk to the adversary, promoting a sense of security, and instilling doubt on behalf

of an adversary. Uninformed security personnel and lighting are examples of deterrence measures.

Emergency – An event or combination of events that have the potential to negatively impact the organization's mission or components of that mission for a period of time and that require immediate response and action to continue normal mission operations.

Exposure – An instance of being exposed to losses from a threat. A weakness or vulnerability can cause an organization to be exposed to possible damages.

Facility – A structure or group of structures in one physical location.

Hybrid Assessment – Aa type of assessment that includes both qualitative and quantitative data and components. Typically, hybrid assessments numerically measure that which can be measured, such as response ties, and assess qualitatively that which cannot.

Infrastructure – The underlying foundation of assets needed for an organization to perform its essential functions and mission-critical operations.

Incandescent Light - is an electric light with a wire filament heated until it glows.

Impact - The extent to which a crime is severe.

Layered Protection – Multiple but integrated levels of security measures to effectively deter, detect, delay and permit response to crime in progress.

Likelihood – The probability that a crime will occur

Mitigation – The act of causing a consequence to have less adverse impact on the organization's mission.

Modus Operandi – The method which an adversary uses to commit a crime or incident.

Project Management – The planning and execution of all aspects of a security project and application of skills, knowledge, and methods to achieve the project's objectives, goals, and requirements on time, within budgetary limitations, and with a high level of quality.

PIDS – Perimeter Intrusion Detection Systems

Protection in Depth – A number of protection devices in sequence.

Physical Protection System – A collection of components or elements to prevent crime.

Qualitative Assessments – A type of assessment that is driven primarily by the assessment subject's characteristics. Qualitative risk assessments are dependent upon the assessor's skills. Scenario-based risk assessments are typically qualitative in nature. The National Terror Alert System is an example of a qualitative threat assessment.

Quantitative Assessment – A type of assessment that is metric based and that assigns numeric values to the risk level. For example, quantitative assessments incorporate security response times and barrier delay times.

Risk – A function of threats and vulnerabilities. Risk is the possibility of asset loss, damage, or destruction as a result of a threat exploiting a specific vulnerability.

Risk Assessment – The process of identifying and prioritizing risks. A quantitative, qualitative, or hybrid assessment that seeks to determine the likelihood that an adversary will successfully exploit a vulnerability and the resulting impact (degree of consequence) to an asset. A risk assessment is the foundation for prioritizing risks in order to effectively implement countermeasures.

Risk Management – A process that seeks to manage threats, vulnerabilities, and risks within an organization. Risk management involves assessing risk, evaluating and selecting security measures to reduce identified risks, and implementing and monitoring the selected measures to ensure that the measures are effective in reducing risk to an acceptable level.

Resilience Capacity – Hardening of security control measures to deter, deflect and delay violent attack.

RFID – Radio Frequency Identification measures

Security Decision Maker – Anyone who has an active role within an organization for asset protection. This term, or its acronym SDM, is used throughout this test since some organizations do not have a formal position of security manager or security director. Risk managers also fall within the security decision maker definition.

Security Risk Analysis – The process of finding the point of intersection between likelihood, impact and vulnerability.

Security Survey – A fact-finding process whereby the assessment team gathers data that reflects the who, what, where, when, and why of an organization's existing operation and facility. The purpose of a security survey is to identify and measure the vulnerabilities to the facility or to specific assets by determining what opportunities exist to exploit current security policies and procedures, physical security equipment, and security personnel.

SLA – Service Level Agreement.

Sterile Zone – An area between physical protection barriers which is free of obstruction and/or movement of people to enable early detection systems to function optimally.

Stress Test – A deliberate but safe action to test an existing security control measure to determine the efficacy and accuracy.

Swiss Cheese Model – The James Reason model of causation.

Threat – Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. Threats are classified as either human or natural.
Threat can also be defined as an adversary's intent, motivation, and capability to attack assets.

Threat Assessment – An evaluation of human actions or natural events that can adversely affect business operations and specific assets. Historical information is a primary source for threat assessments, including past criminal and terrorist events. Crime analysis is a quantitative example of a threat assessment, while terrorism threat analysis is normally qualitative.

Tollgate - A standardised control point where the project phase is reviewed and/or audited and approved (or not) to continue with the next phase.

Vulnerability – Weakness or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. Vulnerabilities include structural, procedural, electronic, human, and other elements that provide opportunities to attack assets.

Vulnerability Assessment - An analysis of security weakness and opportunities for adversarial exploitation. A security survey is the fundamental tool for collecting information used in the vulnerability assessment. A vulnerability assessment is sometimes referred to as a security vulnerability assessment, or SVA for short.