Request for Proposal [RFP]
for Security Personnel – Operations Centre

Copperleaf Country Estate
[Copperleaf]

Document Control

Document Information

	Information
Document ID	*C19/2021 – Operations Centre Management*
Document Owner	*Copperleaf Country Estate*
Issue Date	*12/04/2021*
Last Saved Date	*15/04/2021*
File Name	*Copperleaf RFP Security Personnel – Operations Centre*

Document History

Version	Issue Date	Changes
[1.0]	*21/03/2021*	*New RFP*
[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 Personnel Services for Copperleaf Country Estate.

1.1 Purpose

The purpose of this document is to inform short-listed suppliers of the detailed information required to enable the **Security Tender Evaluation Committee [STEC]** 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 General Manager, and 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 **[STEC]** Team will then review the supplier proposal against a set of predefined criteria and rate the proposal on its ability to satisfy the requirements stated in this document under **section 3 [Requirements Statement].**

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:

Mr. Lance Camphor (Security Manager)
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-mail 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 ☐ Supplier ☐

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.
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 security personnel 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:

The number of years of providing Security Officering in each market segment,
Average number of years each staff member has been with the company,
Level of knowledge of industry,
Level of knowledge of service offered, and
Level of expertise in the service 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 posts. The supplier should review the security posts location to determine what would be required to detect the threats mentioned in **section 3.1.2. from the operations centre**

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.**

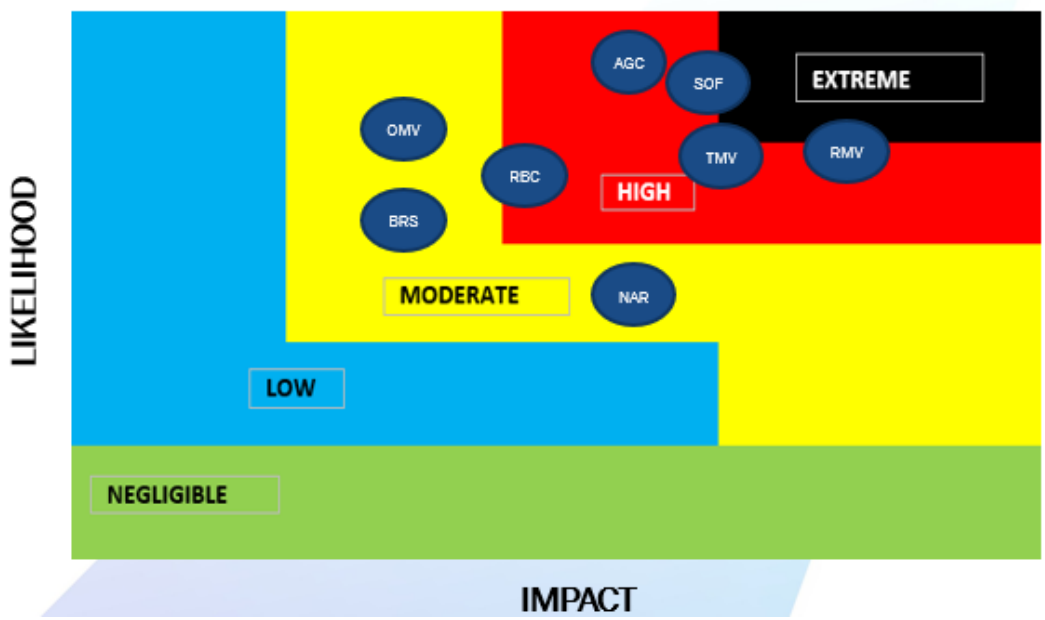

Figure 1: Risk Matrix of probable crime.

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 – SECURITY SERVICE – GENERAL

3.2 PART B – SECURITY SERVICE – GENERAL

3.2.1 Premises (Site) Assessment

Location

The supplier should conduct an **on - site assessment and attend the compulsory briefing** to determine the appropriate fit for purpose security personnel for the Operations Centre requirements.

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

Modus Operandi

The supplier should ensure that the potential threats mentioned in **Part A** of this section are able to be observed by Operations Centre personnel, detected and the correct response initiated.

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 assessment

The supplier should assess and include in the proposal the best fit of the level of security personnel to mitigate the threats mentioned, but not exceeding excessive cost.

Security Officers – All Levels

Service provider shall provide uniformed security services in the operations centre at Copperleaf on a 24 hour-a-day, 7 day-a-week basis, or as otherwise indicated per the site specifications.

Contract security personnel will provide a variety of service, implementing Copperleaf security objectives according to policies and procedures which may include but is not limited to the following general tasks:

- visitor and building employee identification verification, incident and daily operating reports, monitoring and responding to base building intrusion detection systems,

- alarms and fire detection equipment, responding as necessary to support other life safety duties as identified in standard operating procedures.

Service provider shall provide appropriate and necessary management and supervision for all Service provider’s employees and shall be solely responsible for instituting and invoking disciplinary action of employees not in compliance with Service provider or estate security rules.

Service provider shall develop a comprehensive Operations Centre Manual documenting both general procedures as well as site-specific responsibilities.

The Operations Centre Manual shall be prepared prior to the commencement of the contract and must be reviewed and approved by Copperleaf management within thirty (30) days from commencement of the Service provider's services to Copperleaf.

All security officers will be required to read and verify they understand the Operations Centre Manual and shall be tested during the Planned Job Training (PJT) period.

Service provider shall ensure hiring, training and administration of motivated and professional employees that meet or exceed both the Service provider's and Copperleaf's key performance indicators [KPI’s].

Service provider is responsible for the daily personal appearance of security personnel.

Service provider shall provide seasonal uniforms and weather-appropriate protective clothing necessary to support continuous performance of contract requirements.

Service provider shall agree to remove from the site, whenever required to do so by Copperleaf, any employee considered by Copperleaf to be unsatisfactory or undesirable to Copperleaf, within the limits of any applicable laws.

Service provider shall administer all cost accounting and billing relative to this contract.

Service provider shall respond as necessary to accommodate additional duty hours as may be requested by Copperleaf.

REQUIREMENTS STATEMENT

PART C – SECURITY OFFICERS – OPERATIONS CENTRE

3.3 PART C – SECURITY PERSONNEL – OPERATIONS CENTRE

3.3.1 General Duties.

The supplier should ensure that Security Personnel in the Copperleaf Operations Centre must be able to perform the following general duties:

Constantly focus and monitor the site activities via [CCTV] or other surveillance systems [Alarms et cetera],

Respond to the intrusion alarm by instructing the security ground force team,

Control certain system remotely such as gate, doors, or other access points,

Ensure high-level vigilance,

Attention to the detail of every activity,

Monitor and report the camera status functionality, reliability and uptime,

Report downtime or failure on cameras immediately,

Ensure the resolution of the video is good or report deterioration immediately,

Ensure that all of the [CCTV] operating system is working (controllers and software) and monitor the built - in test systems,

Ensure the recording and retrieval system is working and monitor the built - in test system,

Keep a record on the daily system check the electronic or manual logbook,

Video feeds from the available cameras must be screened every ten minutes,

Video patrolling is the systematic monitoring of certain areas of the estate.

Visual patrolling by camera of the designated routes and sequences of the cameras is required,

Video patrolling is dedicated surveillance to check areas of potential threats as well as potential vulnerabilities. This technique is usually set for the control room supervisor in cooperation with the security manager.

Copperleaf will provide a list of areas for critical monitoring through video patrols.

These would typically be:

Vulnerable or critical areas

Remote and low activity areas,

Areas not covered by security officer foot patrols.

The monitoring of live events,

While tracking a live incident Operations Centre personnel should do the following things:

Track the available camera feeds to monitor the location and activities of the adversaries or parties involved,

Report the incident location and adversary to the supervisor,

Be vigilant to further safety and security threats during the ongoing incident.

Effective communication during live incident tracking is an important part of the incident response.

If the incident requires further investigation, the [CCTV] operator may need to retrieve the recorded footage from the backup.

3.3.2 Surveillance Duties.

The supplier must ensure suitability of personnel for a [CCTV] environment.

The qualities required is based on having the observation and visual analysis skills to view, analyse and identify issues occurring on a screen.

The supplier should ensure that before placement their personnel are the subject of the **Surveillance and Monitoring Assessment Excercise** [SAMAE].

Supplier personnel should meet a minimum standard to be acceptable or otherwise will be rejected.

In addition, the supplier should ensure an assessment and comment on the following personality characteristics:

Emotional stability and consistency,
Conscientiousness,
Tough minded and willing to take decisions that can impact on others,
Not taking things at face value or for granted,
Insightful on people and social behaviour,
Willing to look at new or different approaches, and
Self - sufficient and self-disciplined.

3.3.3 Code of Conduct

General Conduct and Breach

The service provider will, and will require their Personnel to, treat all persons humanely and with respect for their dignity and privacy and will report any breach of this Code to Copperleaf. Any breach will be reported via the Incident Reporting Procedure.

Requirements for the Use of Force

The service provider will adopt Rules for the Use of Force consistent with applicable law and the minimum requirements contained in the section on Use of Force in this Code.

Refer to the Criminal Procedure Act 51/1977. Section 49 amended.

Use of Force

Service provider will require their Personnel to take all reasonable steps to avoid the use of force. If force is used, it shall be in a manner consistent with applicable law. In no case shall the use of force exceed what is strictly necessary and should be proportionate to the immediate threat posed and appropriate to the situation.

Service provider will require that their Personnel not use firearms against persons except in self-defence or defence of others against the imminent threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life.

To the extent that Personnel are formally authorized to assist in the exercise of a state's law enforcement authority. Refer to the Criminal Procedure Act 51/1977.

Detention and Arrest

Service provider will require that their Personnel, treat all detained persons humanely and consistently with their status and protections under applicable human rights law or international humanitarian law, including in particular prohibitions on torture or other cruel, inhuman or degrading treatment or punishment.

Refer to the Criminal Procedure Act 51/1977. Section 42, 50 and 47.

Apprehending Persons

Service provider will, and will require their Personnel to, not take or hold any persons except when apprehending persons to defend themselves or others against an imminent threat of violence, or following an attack or crime committed by such persons against Company Personnel, or against clients or property under their protection, pending the handover of such detained persons to the Competent Authority at the earliest opportunity. Any such apprehension must be consistent with applicable national or international law and be reported to the Client without delay. Signatory Companies will, and will require that their Personnel to, treat all apprehended persons humanely and consistent with their status and protections under applicable human rights law or international humanitarian law, including in particular prohibitions on torture or other cruel, inhuman or degrading treatment or punishment.

Refer to the Criminal Procedure Act 51/1977. Also refer to SERVICE PROVIDER Individual Safety standards.

Prohibition of Torture or Other Cruel, Inhuman or Degrading Treatment or Punishment

Service provider will not, and will require that their Personnel not, engage in torture or other cruel, inhuman or degrading treatment or punishment. For the avoidance of doubt, torture and other cruel, inhuman or degrading treatment or punishment, as referred to here, includes conduct by a private entity which would constitute torture or other cruel, inhuman or degrading treatment or punishment if committed by a public official.

Contractual obligations, superior orders or exceptional circumstances such as an armed conflict or an imminent armed conflict, a threat to national or international security, internal political instability, or any other public emergency, will never be a justification for engaging in torture or other cruel, inhuman or degrading treatment or punishment.

Service provider will, and will require that their Personnel, report any acts of torture or other cruel, inhuman or degrading treatment or punishment, known to them, or of which they have reasonable suspicion. Such reports will be made to the Client and one or more of the following: the competent authorities in the country where the acts took place, the country of nationality of the victim, or the country of nationality of the perpetrator.

Sexual Exploitation and Abuse or Gender-Based Violence

Service provider will not benefit from, nor allow their Personnel to engage in or benefit from, sexual exploitation (including, for these purposes, prostitution) and abuse or gender-based violence or crimes, either within the Company or externally, including rape, sexual harassment, or any other form of sexual abuse or violence. Signatory Companies will, and will require their Personnel to, remain vigilant for all instances of sexual or gender-based violence and, where discovered, report such instances to competent authorities and/or to the displayed reporting telephone hotline number.

Discrimination

Service Provider will not, and will require that their Personnel do not, discriminate on grounds of race, colour, sex, religion, age, social origin, social status, indigenous status, disability, or sexual orientation when hiring Personnel and will select Personnel on the basis of the inherent requirements of the contract.

Identification and Registering

Service provider to the extent consistent with reasonable security requirements and the safety of civilians, their Personnel and Clients, will:

require all Personnel to be individually identifiable whenever they are carrying out activities in discharge of their contractual responsibilities. Refer to the Private Security Industry Regulatory Act (PSIRA Act);
all Service provider Personnel are required to carry the PSIRA Registration Card.

ensure that their vehicles are registered and licensed with the relevant national authorities whenever they are carrying out activities in discharge of their contractual responsibilities; and

will ensure that all hazardous materials are registered and licensed with the relevant national authorities.

Conduct during Crowd Management, Intervention and Response Tactics

Crowd management, albeit a legal or an illegal event remains the duty of the South African Police Force.

Service provider is charged to only protect the estate assets against any threat and to support the South African Police Services by monitoring, assessing and providing information about the crowd behaviour.

Selection and Vetting of Personnel

Service provider will exercise due diligence in the selection of Personnel, including verifiable vetting and on-going performance review of their Personnel. Service provider will only hire individuals with the requisite qualifications as defined by the applicable contract, applicable national law and industry standards, and likelihood to comply with the principles contained in this Code.

Service provider will not hire individuals under the age of 18 years to carry out Security Services.

Service provider will assess and ensure the continued ability of Personnel to perform their duties in accordance with the principles of this Code and will ensure that they meet appropriate physical fitness standards, by issuing a fitness certificate from the Occupational Health Practitioner annually at the beginning of each financial year. An assessment for mental fitness should also be done annually.

Service provider will establish and maintain internal policies and procedures to determine the suitability of applicants, or Personnel, to carry weapons as part of their duties. At a minimum, this will include checks that they have not:

been convicted of a crime that would indicate that the individual lacks the character and fitness to perform security services pursuant to the principles of this Code;

been dishonourably discharged;

had other employment or engagement contracts terminated for documented violations of one or more of the principles contained in this Code; or

had a history of other conduct that, according to an objectively reasonable standard, brings into question their fitness to carry a weapon.

For the purposes of this paragraph, disqualifying crimes may include all crimes classified under the Schedule 1 and 2 of the Criminal Procedure Act 51/1977, but are not limited to, battery, murder, arson, fraud, rape, sexual abuse, organized crime, bribery, corruption, perjury, torture, kidnapping, drug trafficking or trafficking in persons. This provision shall not override any law restricting whether a crime may be considered in evaluating an applicant. Nothing in this section would prohibit a Company from utilizing more stringent criteria.

Service provider will require all applicants to authorize access to prior employment records and available Government records as a condition for employment or engagement. This includes records relating to posts held with the military, police or public or Private Security Providers. Moreover, Signatory Companies will, consistent with applicable national law, require all Personnel to agree to participate in internal investigations and disciplinary procedures as well as in any public investigations conducted by competent authorities, except where prohibited by law.

Selection and Vetting of Subcontractors

Service provider will exercise due diligence in the selection, vetting and on-going performance review of all subcontractors performing Security Services.

In accordance with the principles of this Code, Service provider will require that their Personnel and all subcontractors and other parties carrying out Security Services under the contract, operate in accordance with the principles contained in this Code and the standards derived from the Code. If a Company contracts with an individual or any other group or entity to perform Security Services, and that individual or group is not able to fulfil the selection, vetting and training principles contained in this Code and the standards derived from the Code, the contracting Company will take reasonable and appropriate steps to ensure that all selection, vetting and training of subcontractor's Personnel is conducted in accordance with the principles contained in this Code and the standards derived from the Code.

Company Policies and Personnel Contracts

Service provider will ensure that their policies on the nature and scope of services they provide, on hiring of Personnel and other relevant Personnel reference materials such as Personnel contracts include appropriate incorporation of this Code and relevant and applicable labour laws. Contract terms and conditions will be clearly communicated and available in a written form to all Personnel in a format and language that is accessible to them.

Service provider will keep employment and service records and reports on all past and present personnel for a period of 7 (seven) years. Service provider will require all Personnel to authorize the access to, and retention of, employment records and available Government records, except where prohibited by law. Such records will be made available to any compliance mechanism established pursuant to this Code or Competent Authority on request, except where prohibited by law.

Service provider will only hold passports, other travel documents, or other identification documents of their Personnel for the shortest period of time reasonable for administrative processing or other legitimate purposes. This paragraph does not prevent a Company from co-operating with law enforcement authorities in the event that a member of their Personnel is under investigation.

Training of Personnel

Service provider will ensure Personnel performing Security Services at induction, and included in their manual, and at recurrent professional training are also made fully aware of the PSIRA Code, and all other applicable international and relevant national laws, including those pertaining to international human rights, international humanitarian law, international criminal law and other relevant criminal law. Service provider will maintain written records adequate to demonstrate attendance and results from all professional training sessions, including from practical exercises.

Management of Weapons

Service provider will acquire and maintain authorizations for the possession and use of any weapons and ammunition required by applicable law.

Service Provider has appointed a responsible person for the management of weapons and to ensure compliance with the Fire Arms Control Act 60/2000.

Service provider will neither, and will require that their Personnel do not, possess nor use weapons or ammunition which is illegal under any applicable law. Service provider will not, and will require that their Personnel not, engage in any illegal weapons transfers and will conduct any weapons transactions in accordance with applicable laws and UN Security Council requirements, including sanctions. Weapons and ammunition will not be altered in any way that contravenes applicable national or international law.

Service provider policies or procedures for management of weapons and ammunitions shall include:

(a) secure storage,
(b) controls over their issue,
(c) records regarding to whom and when weapons are issued,
(d) identification and accounting of all ammunition, and
(e) verifiable and proper disposal.

Refer to the Fire Arms Control Act 60/2000:

Weapons Training

Service provider will require that:

(a) Personnel who are to carry weapons will be granted authorization to do so only on completion or verification of appropriate training with regard to the type and model of weapon they will carry. Personnel will not operate with a weapon until they have successfully completed weapon-specific training.

(b) Personnel carrying weapons must receive regular, verifiable and recurrent training specific to the weapons they carry and rules for the use of force.

(c) Personnel carrying weapons must receive appropriate training in regard to rules on the use of force.

Refer to the Fire Arms Control Act 60/2000:

Incident Reporting

Service provider will prepare an incident report documenting any incident involving its personnel that involves the use of any weapon, which includes the firing of weapons under any circumstance (except authorized training), any escalation of force, damage to equipment or injury to persons, attacks, criminal acts, traffic accidents, incidents involving other security forces and will conduct an internal inquiry in order to determine the following:

(a) time and location of the incident;

(b) identity and nationality of any persons involved including their addresses and other contact details;

(c) injuries/damage sustained;

(d) the type of weapon involved;

(e) the number of rounds fired (if applicable);

(f) circumstances leading up to the incident; and

(g) any measures taken by Service provider in response to it.

Upon completion of the inquiry, Service provider will where so required, produce in writing an incident report.

Safe and Healthy Working Environment

Service provider will strive to provide a safe and healthy working environment, recognizing the possible inherent dangers and limitations presented by the local environment. Service provider will ensure that reasonable precautions are taken to protect relevant staff in high-risk or life - threatening operations.

These will include:

a) assessing risks of injury to Personnel as well as the risks to the local population generated by the activities of Service provider and/or Personnel;

b) assessing the level of experience of personnel required to attend at a particular situation;

c) providing hostile environment training;

d) providing adequate protective equipment, appropriate weapons and ammunition, and medical support; and

e) adopting policies which support a safe and healthy working environment within the Company, such as policies which address psychological health, deter work-place violence, misconduct, alcohol and drug abuse, sexual harassment and other improper behaviour.

Harassment

Service provider will not tolerate harassment and abuse of co-workers by their Personnel. This includes all forms of harassment that infringes human rights as well as sexual harassment.

Grievance Procedures

Service provider will establish grievance procedures to address claims alleging failure by the Company to respect the principles contained in this Code brought by Personnel or by third parties.

Service provider will:

a. establish procedures including a displayed hotline number for their Personnel and for third parties to report allegations of improper and/or illegal conduct to designated Personnel, including such acts or omissions that would violate the principles contained in this Code. Procedures must be fair, accessible and offer effective remedies, including recommendations for the prevention of recurrence. They shall also facilitate reporting by persons with reason to believe that improper or illegal conduct, or a violation of this Code, has occurred or is about to occur, of such conduct, to designated individuals within a Company and, where appropriate, to competent authorities;

b. investigate allegations promptly, impartially and with due consideration to confidentiality;

c. keep records about any such allegations, findings or disciplinary measures. Except where prohibited or protected by applicable law, such records should be made available to a Competent Authority on request;

d. cooperate with official investigations, and not participate in or tolerate from their Personnel, the impeding of witnesses, testimony or investigations;

e. take appropriate disciplinary action, which could include termination of employment in case of a finding of such violations or unlawful behaviour; and

f. ensure that their Personnel who report wrongdoings in good faith are provided protection against any retaliation for making such reports, such as shielding them from unwarranted or otherwise inappropriate disciplinary measures, and that matters raised are examined and acted upon without undue delay.

No provision in this Code should be interpreted as replacing any contractual requirements or specific Company policies or procedures for reporting wrongdoing.

REQUIREMENTS STATEMENT

PART D – SERVICE COST SCHEDULE AND ADMINISTRATION

3.4 PART D – SERVICE COST SCHEDULE AND ADMINISTRATION

3.4.1 Contract Administration

The Day-to-day communication on matters relating to the contract between Copperleaf and the Supplier for the Operations Centre shall be between the Security Manager for Copperleaf and the Contract Manager of the supplier,

Supplier shall submit monthly invoices within 15 days of the close of a month for the prior month's services.

Supplier shall ensure that all invoices are accurate and shall maintain adequate data to support the accuracy of each invoice. Supplier shall provide Copperleaf with sufficient data to support their invoice upon request.

3.4.2 Schedule of Pricing

Supplier is required to submit a detailed schedule of pricing,

Supplier is required to ensure compliance to the most current contract pricing guideline for the magisterial area in which Copperleaf is located. As published by the Private Security Industry Regulatory Authority (PSIRA),

The schedule should indicate every personnel position proposed for Copperleaf,

The schedule should include a breakdown of costs proposed by the supplier, and

The calculations should include relief security officers.

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.

3.4.3 Duty Roster

Supplier is required to submit a detailed duty roster to encapsulate all the services proposed for 24 hours, daily, monthly to cover an entire year,

The duty roster should indicate every personnel position proposed for Copperleaf,

The duty roster should include relief security officers.

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.

Asset – People, property and information. People may include employees and customers along with other invited persons such as suppliers 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.

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.

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

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

Operations Centre – The central security facility for monitoring, command and control of all security activities on the premises.

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.

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.

SAMAE – Surveillance and Monitoring Assessment Exercise.

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.