SECTION 3: TECHNICAL SPECIFICATIONS

4 TECHNICAL AND GENERAL RESPONSIBILITIES

4.1 INTRODUCTION

The technical specifications set out below are key considerations of the technical requirements required for this RFI.

4.1.1 The University of Johannesburg requires a comprehensive protection and response service for its officials and non-officials (e.g., students) for business purposes. The service provider must be trained in accordance with regulatory and industry standards. Providers are required to deliver services on a scheduled basis, which includes but is not limited to:

- Access Control;
- Protection of property,
- Detection and resolution of security and safety breaches

4.1.2 The service includes scheduled deployments based on threats detected, which may impact University operations.

- Provision of screened and appropriately qualified staff;
- Provision of necessary tools of the trade for the above personnel;
- Management of the above personnel;
- Coordinate with UJ Protection Services personnel in the areas of operation;
- Coordinate all operational meetings with relevant UJ and external stakeholders;
- Provision of monthly and ad-hoc reports on activities.

4.1.3 The University of Johannesburg also requires Security Service providers to deploy trained Security Personnel to perform security duties at the premises occupied by the University of Johannesburg officials on a scheduled or ad-hoc basis.

- Deployment of officers at designated sites;
- Deployment of relief officers at designated sites;
- Management and supervision of all officers deployed;
- Preliminary investigations of incidents and evidence gathering;
- Conduct regular risk assessments and propose mitigation/improvement measures.

4.1.4 The University of Johannesburg also requires Security Service providers to outline their unique value proposition related to the provision and management of people, processes and technologies to protect UJ personnel and property.

- Outline their strategies for the prevention, detection and deterrence of security breaches. Furthermore, the approach to investigations, evidence handling and incident management/response.
- The service provider must outline their strategies and approaches to quality management and industry standards.
- The contractor must propose any recommended best practices and/or rules that must be applied, implemented and enforced.
- Consider economies of scale that could be achieved across various facilities and buildings, the costs need to be provided for each stand-alone facility or building,
- Outline strategies to increase workforce effectiveness, efficiencies, and client centricity.

4.1.5 The prospective service provider **must** comply with the regulations listed below:

- Private Security Industry Regulation Act 56 of 2001:
- PSIRA code of conduct.
- The application of the Control of Access to Public Premises and Vehicle Act, 1985, Sections 2, 3 and 4, as well as C5.
- The application of the Criminal Procedure Act, Act 51 of 1977,
- Protection of Information Act 84 of 1982.
- Occupational Health and Safety Act 85 of 1993 and all other relevant SA legislation.
- The Safety at Sports and Recreational Events Act 2 of 2010 (SASREA)
- The Protection of Personal Information Act, 2013 (POPIA)
- The Promotion of Access to Information Act 2 of 2000