National Integrated Cyberinfrastructure System (NICIS):

South African National Research Network (SANReN) Network Security Grant

---

Call for Applications for SANReN Funding

Prepared by
SANReN
Version 2.0

May 2019

Contents

1 Background

The freedom and opportunities that the Internet brings to the modern world unfortunately also enable criminal elements to freely operate and attack commercial, private and state Information and Communication Technology (ICT) systems. Compared to traditional crime, Cyber crime is not only considerably cheaper to undertake, but is also not constrained to physical locations. This low barrier-to-entry has resulted in a massive growth in Cyber-related crime in recent times. Cyber attacks have real-world consequences ranging from Intellectual Property (IP) theft to endangering human life by compromising critical systems such as nuclear power stations. In the domain of telecommunication networking, the vastness and complexity of interconnectivity have provided a platform for Cyber criminals to not only operate inconspicuously, but also to effect massive impact on network availability with very little effort.

Developing technologies to facilitate attack detection and risk mitigation is an on-going global effort. These technologies include attack sensors, such as Intrusion Detection Systems (IDS), Honeypots, Firewalls, Network Telescopes and various system logging platforms. Each of these technologies is highly specialized and may detect a myriad of events within a network, as well as possibly identify the sources of such attacks and intrusion. Although some of these systems are mature, significant scope exists for directed research in the development, application and methods used by such technologies, specifically in the domain of Network Security.

The South African National Research Network (SANReN) is a high-speed network dedicated to science, research, education and innovation traffic and has been rolled-out in a phased manner since 2007. It is part of a comprehensive South African government approach to a National Integrated Cyberinfrastructure System (NICIS) to ensure successful participation of South African researchers and scientists in the global knowledge production effort. SANReN works in close collaboration with the Tertiary Research and Education Network of South Africa (TENET) that operates the SANReN network. The South African National Research and Education Network (SA NREN), which constitutes the joint efforts and investments of SANReN and TENET, recently implemented a Computer Security Incidence Response Team (CSIRT) to address the Cybersecurity needs of the SA NREN and its beneficiaries. The efforts of this CSIRT is split such that proactive services reside with SANReN and reactive services reside with TENET.

This call, directed at all South African public universities, is to grow the capabilities of the SA NREN CSIRT through directed and targeted research into network security, as well as developing human capacity in this domain.

2 Scope of the funding instrument

SANReN herewith requests proposals from South African public universities to host a grant programme that is designed to assist post-graduate students performing research in the fields of network security. This grant programme is aimed at:

- supporting applied research in the field of network security, with a specific focus on the application thereof in the NREN domain
- developing a pipeline of graduates skilled and capable in network security

Funding will be awarded to the university that is deemed to be most capable of leading Masters and PhD level graduate students, as well as post-doctoral researchers in the field of network security.

3 Research Focus Areas

The focus of the research performed by grant-holding Masters and PhD students needs to align to SANReN's strategic direction in the domain of network security, which ultimately should lead to the identification and mitigation of Cyber security threats on the SANReN network. These include, but is not limited to the following:

- Policy design and implementation of network security for NRENs.
- Advanced network sensors to pro-activaly identify network security threats.
- Inter-NREN network security threat mitigation.
- Skills development for network security specialists in South Africa.
- NREN network infrastructure hardening.
- Threat intelligence correlation and aggregation, inter- and intra-NREN.
- Impact of exploited network security threats on the reputation of the NREN.
- Evaluation of the effectiveness of Cyber security awareness methodologies.

4 Eligibility Criteria

All public South African universities with an existing capability in network security related research and training are eligible to apply to host the SANReN network security grant programme. The academic(s) that will lead the grant programme at the successful university need to:

- Have a proven track record of in research in the domain of network security and will need to provide evidence in the form of peer reviewed publications, patents, technical reports, of past experience.
- Have at least one academic with a Doctoral degree qualification.
- Have a track record in postgraduate student training for a minimum period of five years.
- Be employed in a permanent full-time position or on a full-time fixed term contract basis for a period of three years for at least the duration of the funding period for the grant programme.

5 Application Requirements

All proposals must include the following information:

- Overview of existing research programme(s) with specific focus in the domain of network security.
- Contact information of the academic staff member that will lead the programme. at the successful university.
- Qualification and research focus area details of all academic staff that will support/participate in the grant programme.
- Details of the support staff that will support the grant programme.
- A list of all publications and other research outputs generated by the academic staff that will support/participate in the grant programme.
- Student supervisory history for research projects in the domain of network security of all academic staffs that will support/participate in the grant programme.
- Availability of specific research infrastructure that will support the hosting of the grant programme.
- A business plan of 5 to 10 pages that provides argumentation for selection, envisaged research deliverables (research outcomes and outputs), potential research tracks and topics, student recruitment plan, 3-year provisional budget and cash flow statement, risk management plan, any other funding sources that could potential augment the SANReN funding, potential collaborations that could be undertaken with other research institutions and universities in support of the grant programme, etc.

- Abridged Curriculum Vitaes (CVs) of all academic staff that will support/participate in the grant programme.

6 Review and Evaluation Process

The criteria for evaluation of applications submitted for the SANReN grant programme in network security is outlined in the table below:

Table 1: Proposal evaluation scoring criteria

Criterion	Details	Weight
Alignment with SANReN strategic direction in network security	Direct alignment with SANReN strategic direction (30%)	40%
	Innovativeness and scientific/technical excellence of the proposed programme (5%)	
	Alignment with national priorities (5%)	
Feasibility of the research proposed programme	Business plan feasibility in terms of (30%): • timelines, • budget, • resourcing, • risks, • potential for successful completion • and attainment of set objectives and outputs.	40%
	Academic staff track record in terms of research outputs. (past papers, student studies completed, staff qualifications) (10%)	
Human Capital Development	Planned HCD outputs (number of PhD students to be supported, number of Masters students to be supported, number of bridging students supported) (5%)	10%
	Number of potential students from designated groups (current and historic students linked to the PI) – (5%)	
Research Outputs and collaboration	Planned research outputs (papers, articles, demonstrators, code) (5%)	10%
	Intra-institutional, regional and national International Private sector (5%)	

Preference will be given to proposals that undertake to award grants to students from designated groups viz. black, female and persons with disabilities, in line with the ministerial guidelines on equity and redress.

The proposal will be evaluated on a six-point scale from 0 to 5. The scores indicate the following with respect to the criterion under review:

Table 2: Scoring for review and evaluation process

Scores	Description
0	**No score:** the proposal fails to address the issue under review or cannot be judged against the criterion due to missing or incomplete information.
1	**Poor:** the proposal provided insufficient information, and/or numerous inconsistencies. Therefore a fair evaluation cannot be conducted. As such this is considered a high risk investment.
2	**Fair:** the proposal partially addresses the requirements. However, some key issues have not been adequately addressed.
3	**Adequate:** the proposal meets the necessary requirements in this section. However, there are some issues that should be addressed by the applicant and institution before an award is made.
4	**Good:** this is a strong proposal that fully addresses all the requirements in this section. However, there are minor issues that the applicant is advised to bear in mind.
5	**Excellent:** this is an exceptionally strong proposal that is well conceptualised and strongly motivated and exceeds all the requirements in this section.

A Grant Programme Adjudication Committee (GPAC), constituted by the CSIR, will adjudicate the proposals received based on the above criteria.

7 Funding

SANReN commits to provide up to R500 000 grant funding per year for three (3) years to be allocated by the successful university to computer science/engineering students performing SANReN approved targeted research into network security. The following maximum financial assistance per student receiving a grant from this programme will apply:

- Masters: R 80 000 per annum for 2 years
- PhD: R 120 000 per annum for 3 years

The successful university will be required to advertise grants from this programme to prospective students nationally in order to reach potential deserving students at all South African Higher Education Institutions (HEIs).

Institutions can motivate to allocate a portion of this funding to hardware and/or software infrastructure that will support grant-holder Masters and PhD students. The maximum value of this equipment/software is not to exceed value of 10% of the total 3-year budget. In addition, grant funding can be used for bridging courses for exceptional students wishing to change their study focus to that of network security.

Post-graduate students that are awarded grants from this programme are expected to spend two to six weeks at the CSIR Pretoria Campus per year, working on SANReN projects related to their respective Masters or PhD research. SANReN will also endeavor to:

- Provide co-supervision support to grant-holder Masters and PhD students during their studies, as required and where feasible.
- Provide access to SANReN infrastructure and data sources to grant-holder Masters and PhD students during their studies, as required and where feasible.

The funding may not be used for the following expenses:

- The acquisition and deployment of high-end Cyber-infrastructure that is readily available from NICIS itself.
- Man-hours spent on conducting, supervising and supporting research by the academic and support staff allocated to this programme by the successful university.
- Subcontracting the proposed grant programme activities to agents or entities that do not form part of the proposal.

8 Reporting, Monitoring and Evaluation

A Grant Programme Governance Committee (GPGC), with membership from SANReN and the successful university, will govern this grant programme. The GPGC will meet twice per year to review new potential grant candidates, select research topics, review the performance of existing candidates, as well as decide on the financial, operational and strategic direction of the programme. The successful university will be required to submit bi-annual progress reports and an annual report in formats to be defined by SANReN.

9 Intellectual Property and Research Outputs

The CSIR and the successful university will retain their respective background Intellectual Property (IP) that might be required during the 3-year duration of the grant programme. Foreground IP generated through the research performed by the grant-holder Masters and PhD students will be shared by the CSIR and winning university, as agreed on in the GPGC on a case-by-case basis, in accordance with the South African Intellectual Property Rights from Publicly Financed Research and Development Act of 2008.

Ownership and custodianship of code and prototypes generated through research performed by grant-holding Masters and PhD students will be agreed on in the GPGC on a case-by-case basis. Any papers or articles generated by these students must, as a minimum, include an acknowledgement to SANReN for the funding provided in support of the research, but ideally include as co-author a SANReN staff member that have actively participated in the writing thereof.

10 Submission of Proposals

Universities that wish to apply for the grant programme can submit their proposals to Dr. Renier van Heerden at renier@sanren.ac.za on or before 1 July 2019.