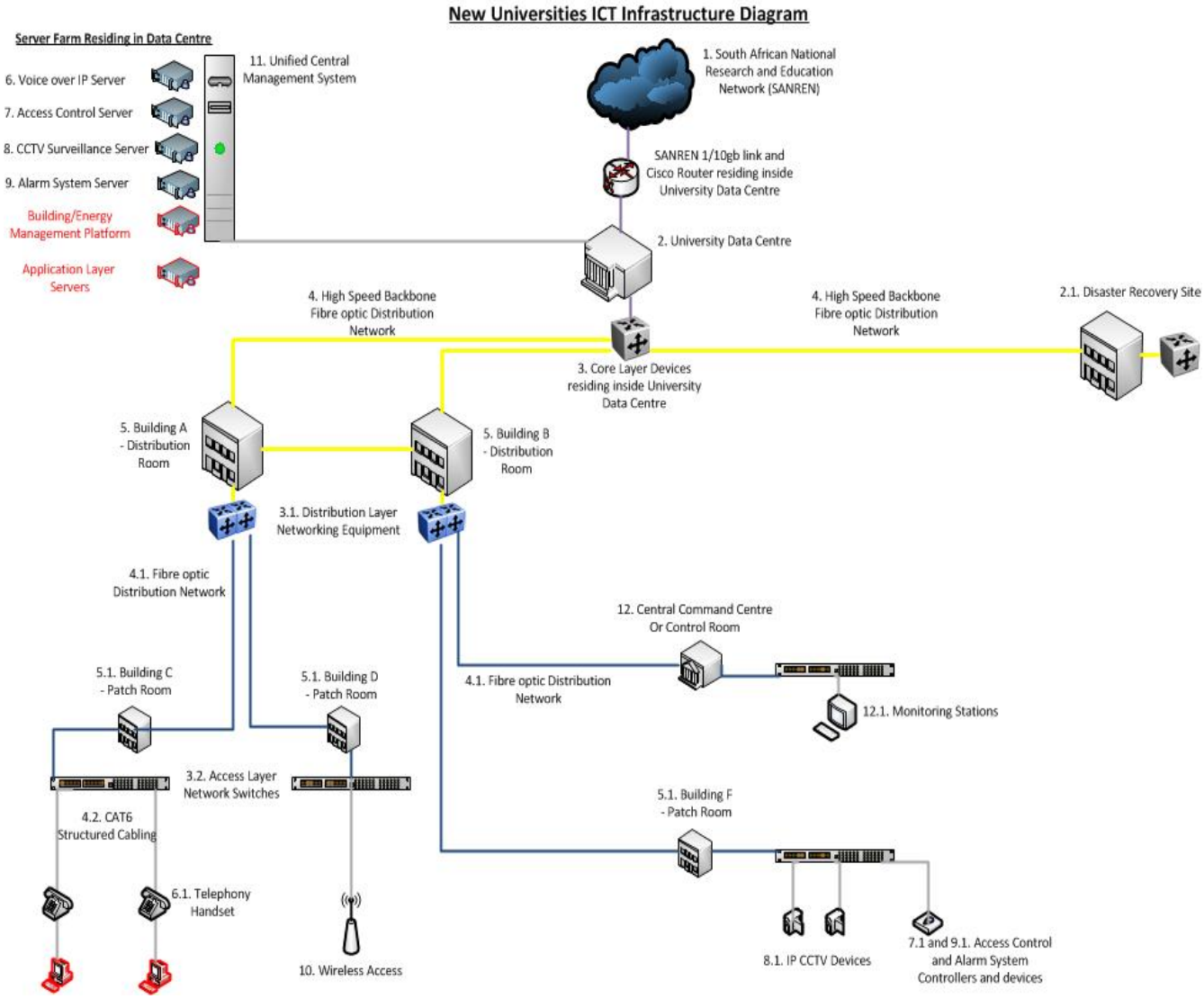
New Universities ICT Report - Kimberley

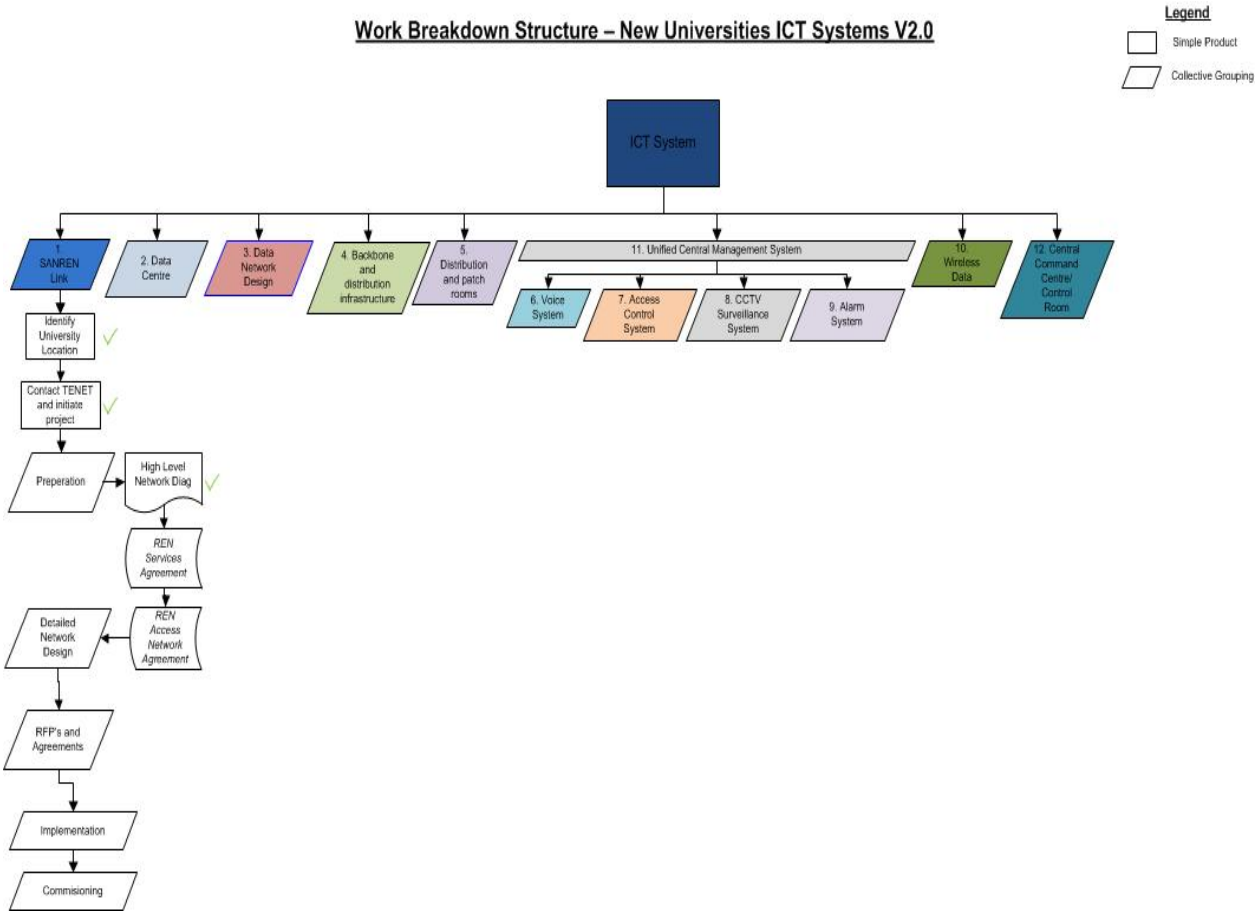
1. Introduction

The term ICT (information and communications technology – or technologies) is an umbrella term that includes any communication device or application. This document speaks to ICT's relating to the Data Network, Telephony system and Electronic Security Systems (Access Control, CCTV and Alarms).

2. Infrastructure Diagram



3. **Work Breakdown Structure**



4. WBS Component Details

4.1 SANReN Data Link

4.1.1 Summary

The South African National Research Network (SANReN) is part of a comprehensive South African government approach to cyber infrastructure to ensure successful participation of South African researchers in the global knowledge production effort. Together with the Centre for High Performance Computing (CHPC) and the Very Large Databases (VLDB) project, SANReN forms a key component of this cyber infrastructure as a core scientific infrastructure for South Africa.

The SANReN is a high-speed network dedicated to research traffic and research into research networking and broadband infrastructures. It is being rolled out in a phased manner and will connect up to 204 sites across the country with research networks hosting over 3 000 research and education organizations from all over the world in the first two phases, which commenced in 2007.

Conceptualization

The SANReN initiative was conceptualized in 2003 in partnership with the then Department of Arts, Culture, Science and Technology. Extensive planning and consultation on the South African approach to high performance computing and research networking were conducted since then. The SANReN and CHPC were discussed in Cabinet and the budget line items as part of the research infrastructure budget of DST were approved and announced during Minister Mangena's budget speech in 2006.

The responsibility for the implementation planning was given to the CSIR Meraka Institute, at that stage already involved with the process of establishing the CHPC, in the beginning of 2006 to ensure a comprehensive and holistic approach to cyber infrastructure development. A three-year contract was signed between the CSIR and DST in 2006 for the implementation and management of this project ending in financial year 2009/10. This includes all aspects of the research, design, planning, implementation and monitoring of the network for the period. The SANReN project subsequently forms part of the approved CSIR Meraka Institute business plans from 2006 onward.

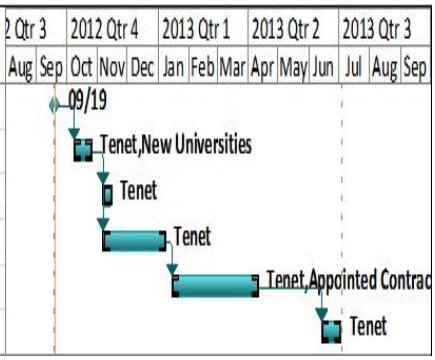
The CSIR has identified TENET as a crucial partner in the deployment of SANReN. TENET currently operates the SANReN network on behalf of the CSIR, and has been intimately involved in the planning of many aspects of the network and further roll-out.

4.1.2 High Level Design

4.1.3 High Level Program

Five month implementation program.

ID	Task Mode	Task Name	Duration	Predecessors	Resource Names
1		Project Initiation	0 days		Martin,Tenet
2		Preparatory Work	14 days	1	Tenet,New Universities
3		Network Design	7 days	2	Tenet
4		RFP's and Agreements	45 days	2	Tenet
5		Project Implementation	63 days	4	Tenet,Appointed Contractor
6		Comissioning	14 days	5	Tenet



4.1.4 Cost Estimate

Item No.	Item Category	Description	Unit Cost	Cost Estimate excl Vat
1	**Bulk Data**			
1.1	Fibre optic connection	Connection to the SANReN Network (Red) - Diverse Route	R 750 000.00	R 750 000.00
		Sub Total:		**R 750 000.00**

4.2 Internal Campus Data Network

4.2.1 Data Centre

We define a data center as a special facility that performs one or more of the following functions:

- A data center physically houses various equipment, such as computers, servers (e.g., web servers, application servers, database servers), switches routers, data storage devices, load balancers, wire cages or closets, vaults, racks, and related equipment.
- Data centers store, manage, process, and exchange digital data and information;
- Provide application services or management for various data processing, such as web hosting internet, intranet, telecommunication and information technology.

4.2.2 Core Networking Layer

The core hardware is typically interconnected to all distribution network hardware and the objective is to ensure that the data traffic continues for the whole network, this is a Layer 3 device

4.2.3 Backbone Fibre Infrastructure

Campus fibre optic backbone interconnecting Core, Distribution and Patch rooms. Single mode OM3 Fibre for Core-Distribution-DR and Multimode Fibre for Distribution-Patch Rooms.

4.2.4 Distribution and Patch Rooms

Distribution points deal with the direct connection from the Core/Data Centre via fibre optic redundantly connected to other distribution points to form a mesh topology. These rooms should be 3x3 m^2 air conditioned with the necessary security but does not require raised flooring.

Each building is then connected from its own patch room via fibre optic to the distribution point. The patch rooms are similar in construction i.e. 3x3m^2 with the necessary security but naturally ventilated. These patch rooms act as the local building distribution for other services like network, access control, cctv and alarms usually.

It is good practice for the distribution and patch rooms to be physically separate areas/rooms but can be in the same building.

The infrastructure deployed within each patch room is dependent on various factors:

- What is the function of the building/area;
- What is the occupation in terms of quantity;
- Who will be occupying the space i.e. student/staff;
- Any special data/connectivity requirements or high secure areas.

4.2.5 Cost Estimate

Item No.	Item Category	Description	Unit Cost	Cost Estimate excl Vat
2	**Internal Data Network**			
2.1	Data Centre	Internal cabling, self-contained pod, UPS	R 4 800 000.00	R 4 800 000.00
2.2	Disaster Recovery Site (2nd Data Centre)	Same as data centre	R 4 800 000.00	R 4 800 000.00
2.3	Basic Services Cloud	Services such as active directory, exchange, dhcp, iis etc.	R 7 000 000.00	R 7 000 000.00
2.4	Core Networking Layer	Firewall, DMZ, Layer 3 Routing Devices, DR Site Routing Equipment	R 7 900 000.00	R 7 900 000.00
2.5	Backbone Fibre Infrastructure	Fibre optic backbone, linking Core and Distribution in mesh topology and Distribution to patch rooms in Star Topology (est. 25km fibre)	R 120.00	R 3 000 000.00
2.6	Distributions (3 Buildings)	Layer 3 routing devices and UPS Units	R 1 520 000.00	R 4 560 000.00
2.7	Patch Rooms and copper distribution (75 Buildings)	Allowance for 48 ports per building, Layer 2 access Switches, Internal Copper Cabling, 3 x Wireless AP's and local UPS units for networking equipment	R 138 000.00	R 10 350 000.00
		Sub Total:		**R 42 410 000.00**

4.3 Telephony System

4.3.1 Summary

Voice over Internet Protocol (VoIP) is a technology that allows you to make voice calls using a single cable data network connection.

4.3.2 Costs Estimate

Item No.	Item Category	Description	Unit Cost	Cost Estimate excl Vat
3	**Voice over IP Telephony Services**			
3.1	Servers	Voice over IP servers with redundancy	R 2 850 000.00	R 2 850 000.00
3.2	Telephone Handsets	Unit price per handset, allowance for 500 units	R 1 650.00	R 825 000.00
		Sub Total:		**R 3 675 000.00**

4.4 Electronic Security Systems

4.4.1 Summary

Electronic Security Systems refers to three components – Access Control, CCTV and Alarm Systems. Refer to Appendix 8.4, a guideline for the deployment of electronic security systems.

4.4.2 Costs Estimate

Item No.	Item Category	Description	Unit Cost	Cost Estimate excl Vat
4	**Electronic Security Systems**			
4.1	Access Control	Access Control Servers and Database Servers $8.6	R 3 298 100.00	R 3 298 100.00
4.1.1		Physical Access Control point as per Security Deployment Guideline. Allowance made for 3 x Access Points per building	R 74 000.00	R 5 550 000.00
4.2	CCTV	CCTV Recording Servers (200 camera capacity) $8.6	R 1 754 400.00	R 1 754 400.00
4.2.1		Unit price per CCTV Camera, allowance for only 2 x Cameras per building	R 11 800.00	R 1 770 000.00
4.3	Alarm Systems	Alarm Monitoring Server	R 1 000 000.00	R 1 000 000.00
4.3.1		Alarmed locations. Allowance made for Basic System per building.	R 18 500.00	R 1 387 500.00
		Sub Total:		**R 14 760 000.00**

5. Risks

Item No.	Risk	Description	Importance
1	SANRen Fibre Optic Link	Delay in the implementation of the SANReN fibre optic could occur if approvals/ way leaves are not dealt with efficiently by Sanral and local municipality.	Moderate
2	Data Network	Only when building designs are done would an over or under estimation be picked up in terms of the number of connections	Moderate

3	Campus Fibre Network	Almost all fibre optic cable from Core-Distribution-Patch rooms run on public roads, approvals and way leaves from local municipality is required.	High
4	Access Control	Only when building designs are done would an over or under estimation be picked up in terms of the number of access control points	Moderate
5	Alarms	Only when building designs are done would an over or under estimation be picked up in terms of the number of alarmed locations	Moderate
6	CCTV	Only when building designs are done would an over or under estimation be picked up in terms of the number of CCTV cameras	Moderate

6. Exclusions

HR Systems

Student management Systems

Financial Systems

Building Management Systems

Audio Visual Systems

Facilities management systems

All Database services

All PC's, Printers

7. Combined Cost Estimate

New Universities ICT Cost Estimate - Kimberley				
Item No.	**Item Category**	**Description**	**Unit Cost**	**Cost Estimate excl Vat**
1	**Bulk Data**			
1.1	Fibre optic connection	Connection to the SANReN Network (Red) - Diverse Route	R 750 000.00	R 750 000.00
		Sub Total:		**R 750 000.00**
2	**Internal Data Network**			
2.1	Data Centre	Internal cabling, self-contained pod, UPS	R 4 800 000.00	R 4 800 000.00
2.2	Disaster Recovery Site (2nd Data Centre)	Same as data centre	R 4 800 000.00	R 4 800 000.00
2.3	Basic Services Cloud	Services such as active directory, exchange, dhcp, iis etc.	R 7 000 000.00	R 7 000 000.00

2.4	Core Networking Layer	Firewall, DMZ, Layer 3 Routing Devices, DR Site Routing Equipment	R 7 900 000.00	R 7 900 000.00
2.5	Backbone Fibre Infrastructure	Fibre optic backbone, linking Core and Distribution in mesh topology and Distribution to patch rooms in Star Topology (est. 25km fibre)	R 120.00	R 3 000 000.00
2.6	Distributions (3 Buildings)	Layer 3 routing devices and UPS Units	R 1 520 000.00	R 4 560 000.00
2.7	Patch Rooms and copper distribution (75 Buildings)	Allowance for 48 ports per building, Layer 2 access Switches, Internal Copper Cabling, 3 x Wireless AP's and local UPS units for networking equipment	R 138 000.00	R 10 350 000.00
		Sub Total:		**R 42 410 000.00**
3	**Voice over IP Telephony Services**			
3.1	Servers	Voice over IP servers with redundancy	R 2 850 000.00	R 2 850 000.00
3.2	Telephone Handsets	Unit price per handset, allowance for 500 units	R 1 650.00	R 825 000.00
		Sub Total:		**R 3 675 000.00**
4	**Electronic Security Systems**			
4.1	Access Control	Access Control Servers and Database Servers $8.6	R 3 298 100.00	R 3 298 100.00
4.1.1		Physical Access Control point as per Security Deployment Guideline. Allowance made for 3 x Access Points per building	R 74 000.00	R 5 550 000.00
4.2	CCTV	CCTV Recording Servers (200 camera capacity) $8.6	R 1 754 400.00	R 1 754 400.00
4.2.1		Unit price per CCTV Camera, allowance for only 2 x Cameras per building	R 11 800.00	R 1 770 000.00
4.3	Alarm Systems	Alarm Monitoring Server	R 1 000 000.00	R 1 000 000.00
4.3.1		Alarmed locations. Allowance made for Basic System per building.	R 18 500.00	R 1 387 500.00
		Sub Total:		**R 14 760 000.00**
		TOTAL:		**R 61 595 000.00**

University of the Witwatersrand, Johannesburg
Technical Security Guidelines (DRAFT)

Classification	Area Type	Intruder alarms	Access Control (electronic)	Intercoms	Surveillance (refer to Camera Use Policy)
Open Space	Parking			Emergancy Contact points within 400m of each other	Required
	Pedestrian				
	Vehicle pathway				
	Gathering place				
	Vehicle booms or gates		•Access reader In and Out • light duty booms or low sliding gate equiped with Saftey sensors • Gate to be configured for "condominium" operation. (auto closing)	Wireless if required	
Campus Perimeter	Vehicle Entrance	Guard houses to be fitted with Panic Button per external door.	• Access reader In and Out • Spike barrier • Delayed secondary exit boom • Electronic lane open/closed signage if any bidirectional lanes	If unmanned then wireless required	Required
	Pedestrian Entrance		• 4 arm full height turnstile • Access reader In & Out • Anti-Pass-Back enabled. required. • Automated side entrance door/gate for wheelchair users		
Building Perimeter	With campus boundary	PIR and Digipad per office on boundary wall - Typically ground floor, first floor and second floor.	No access to exterior of campus.		Not required
	With Access Control		• Access reader In & Out • Hold open devices and door closures or doors to be closed at all times, can be unlocked with card or schedule. • Emergency Door Release button (green Box) with lift flap and lead seal. • Door prop and force alarms to be monitored and responded to by Campus Control.	Up to four Points: Wireless Intercom more than 4: Internal telephone	Required
	Fire Escape Doors		• Emergency Door Release • Alarms to be monitored, responded to and reset by Campus Control. • If Campus boundary: include 2 minute delay, otherwise no delay.		Required
	Without Access Control		Only existing buildings. All new building or renovations should comply with the above.		Required
Lift			• Access Control inside CAB. • If additional security required or 3 floors or less, then Call button Reader.	Emergency contact intercom supplied with lift and linked to Campus Control	Not Required
Building Passage	With Access Control		• Access reader In, • push button exit	Up to four Points: Wireless Intercom more than 4: Internal telephone	Recommended
	Without Access Control				
Office Reception area/desk		Digipad and PIR Panic Button Keypad	Remote release for passage door	Typically has a handset for intercom	Recommended if foyer
Building Lavatory					Required
Building Office	with windows that are accessible from the outside of the building using up to a 4 meter ladder - Typically ground floor and first floor	PIR with Digipad per Office.			Not Recommended
	with windows not easily accessed from the outside of the building- Typically second floor and higher	Not required if passage is equipped with Access Control and Cameras as per Building Passage			
	Boardroom/meeting room				
PC Lab	Entrance	Digipad	• UG: Turnstile required • PG >= 20 PCs, Access IN and Out on Door. • PG >= 30 PCs, turnstile required • If Turnstile, then wheelchair access required • 2 minute delay on Emergency Escape, Fire Detection to bypass delay	Up to four Points: Wireless Intercom more than 4: Internal telephone	Required
	Interior	PIRs	Server/network rooms Access IN		Required
Laboratory	Entrance	Digipad	• Access Reader In • push button exit on Main door. • Additonal doors are slave doors	Up to four Points: Wireless Intercom more than 4: Internal telephone	Required
	Interior	PIRs			Required
Library	Entrance	Digipad and PIRs	• turnstile • Access reader In & Out • Anti-Pass-Back enabled. required. • Automated side entrance door/gate for wheelchair users • Book theft detection integration • 2 minute delay on Emergency Escape	Up to four Points: Wireless Intercom more than 4: Internal telephone	Required
	Work Spaces (24 Hour)	Digipad and PIRs			

University of the Witwatersrand, Johannesburg
Technical Security Guidelines (DRAFT)

Classification	Area Type	Intruder alarms	Access Control (electronic)	Intercoms	Surveillance (refer to Camera Use Policy)
	Work Spaces (Limited Time)	Digipad and PIRs			
	Other Areas (Book shelves, etc)	Digipad			
Auditorium	**Entrance**	Digipad and PIRs	• Access Reader In • push button exit on Main door. • Additonal doors are slave doors		Required
	Podium		• Access Reader to control Equipment and AC/Lights shutoff • Access Reader to roving microphone		
	Audio Visual Room	Digipad and PIR	Access In, push button Out		Required if external to venue
	Fixed Projector	Magna Pull			
	Chemical Storage facility	Digipad and PIRs	• Access Reader In • push button exit.		Required
Infrastructure	**Network Patch room**		• Access Reader In • push button exit.		Not Required
	Server Room	Digipad and PIR	• Access In, • Push button Out • Fire Suppression integration		Required
	Data Centre	Digipad and PIR	• Access In and Out • Fire Suppression integration • 2 minute delay on Emergency Escape	Up to four Points: Wireless Intercom more than 4: Internal telephone	
	Plant and Equipment		• Access Reader with Keypad In, • Push button Out		
	Electrical Sub Station		• Access Reader with Keypad In, • Push button Out		
	Roof Access		Access Rreader In & Out		
	Residence Hall Main Entrance		• Turnstile or Cubicle. • If turnstile wheelchair/luggage door required. • If Cubicle then it must accommodate a wheelchair.	Up to four Points: Wireless Intercom more than 4: Internal telephone	Required

About TENET

1 June 2012

1. Purpose, constitution and organisation

Names and primary purpose: TENET's registered full name appears in the header of this document. "TENET" is a registered short name.

TENET was created in August 2000 by the public universities of South Africa to function as the organisational home of and vehicle for collaborative internetworking by universities, science councils and associated support institutions ("the institutions"). TENET has fulfilled this mandate for the past 11 years and is recognised as the *national research and education network* ("NREN") of South Africa.

TENET does not provide services to commercial entities and does not participate in the commercial market for Internet services.

Constitution and other legalities: TENET was originally incorporated under the Companies Act as what was then called a "Section 21 Company". Recent amendments to the Companies Act mean that TENET is now incorporated as a so-called "non-profit company". It is recognised by SARS as a Public Benefit Organisation that is exempt from income tax.

TENET holds electronic communications licenses from ICASA that fully permit TENET to build and operate electronic communications networks, including optical fibre networks, and to provide electronic communications services to other parties.

All public universities and science councils qualify to participate in TENET's governance as members. TENET is managed by a Chairperson and Board of Directors who are elected by the members.

TENET is a founder member of the well known UbuntuNet Alliance, the *regional* research and education network organisation for eastern and southern Africa. UbuntuNet provides TENET (and other African NRENs) with connectivity in London and Amsterdam to other research and education networks of the World and to the Internet worldwide.

Organisation: TENET is a membership-based nonprofit company whose members are the public universities and some of the science councils. The members appoint the chairperson and the directors. Operational control is delegated to the CEO who is supported by three other executive officers and eight other staff members. TENET makes substantial use of expert consultants.

Eight members of staff, including the executive officers, are based at the head office in Wynberg, Cape Town. The other four staff members are based at TENET's Network Operations Centre in Johannesburg.

2. Service provision

Specialised service provider: Currently TENET provides Internet and related services to 140 campuses of 54 institutions. TENET enters into a formal service agreement (called the "REN Service Agreement") with each institution, which sets out TENET service level obligations, specifies ordering, billing and payment processes, and binds the institutions to compliance with Acceptable Use and Connection policies.

Cost recovery: TENET recovers the full cost of service delivery through service charges that its Board sets from time to time. In aggregate, service charges billed to institutions during 2010 amounted to almost R100m.

TENET enjoys no recurring subvention of its costs by Government or donors.

3. Network Infrastructure

SANReN is the core: The core of the network that TENET operates today is the South Africa National Research Network ("SANReN") that has been deployed over the past five years by the Meraka Institute of the CSIR under contract to the DST.

Importantly, while TENET bears the costs of operating SANReN, the costs of deploying and maintaining SANReN are borne by the DST through Meraka and are not recovered from the institutions.

SANReN comprises a national backbone, several metropolitan rings, and some dedicated long-haul circuits to reach important research installations. These components are described briefly in the indented sections that follow.

> ***SANReN backbone:*** The SANReN national backbone was provided by Telkom SA commissioned in December 2009. It comprises a 10 Gbps, 7-stretch backbone ring interconnecting nodes at Pretoria, Johannesburg, Bloemfontein, Cape Town, Port Elizabeth, East London and Durban (and back to Pretoria);
>
> ***SANReN metropolitan networks:*** Dark Fibre Africa supplied SANReN's optical fibre ring networks in Johannesburg, Pretoria, Cape Town and Durban that were commissioned during 2010. In aggregate connect some 90 urban campuses to the backbone.
>
> ***Dedicated access circuits:*** SANReN includes 10 Gbps long-haul circuits to the radio-astronomy and space operations centres at Hartebeeshoek; the astronomical observatory at Sutherland and the developing radio-astronomy site at Carnarvon.

Additional campus access circuits: TENET itself provides access circuits to many campuses. These include optical fibre access circuits that connect six campuses, each to its nearest SANReN node, including the main campuses of MINTEK, Monash SA and the University of Zululand, and major satellite campuses of UJ Soweto, UNISA Florida and WITS Baragwanath. TENET connects nine campuses via low-speed rented access circuits, and some 40 smaller sites via ADSL lines and a shared connection between Telkom's ADSL network and the TENET gateway in Johannesburg.

International bandwidth: "International bandwidth" refers to connectivity between South Africa and any major Internet exchange on another continent. TENET owns and uses bandwidth on the SEACOM submarine cable between the SEACOM Landing Station at Mtunzini and Telecity, London. Two different circuits that follow different routes are used to connect the Mtunzini Landing Station to the SANReN node at Durban.

When submarine cables break it can take several weeks to repair them. SEACOM has had two such long outages. For this reason TENET purchases, for a substantial monthly cost, an insurance in the form of "disaster-recovery Internet transit", delivered at TENET's Reefhead Gateway via a different submarine cable.

> ***TENET's SEACOM capacity:*** In 2007 TENET purchased the indefeasible right of use ("IRU"), for the life of the cable, to a 10 Gbps circuit to London on the then recently announced SEACOM cable system. The SEACOM IRU is a long-lived capital asset, the $20m purchase price of which was financed by 27 of the institutions.
>
> The circuit was commissioned in July 2009, and from Jan 2010, when the SANReN backbone was also available, it has enabled the institutions to afford dramatically greater international bandwidths.

Worldwide peering and transit: TENET is an honorary member of the South African Internet Service Providers Association (ISPA) and has peering interconnections with most South African ISPs at ISPA's Internet Exchanges in Johannesburg and Cape Town.

TENET secures interconnectivity with other NRENs and with the Internet worldwide through the London and Amsterdam gateways of the UbuntuNet Alliance for Research and Education Networking (UbuntuNet), which is the regional research and education network for Eastern and Southern Africa. At these gateways UbuntuNet has interconnections with the European research and education network, GÉANT, and hence with other NRENs worldwide, and also to the major London and Amsterdam Internet Exchanges.

TENET is a founding Member of UbuntuNet and actively supports and promotes UbuntuNet's role as a regional research and education network.

4. Network operations

TENET operates the entire infrastructure described in the previous section, including all campus terminating devices, core switches and routers, and the gateways in Cape Town and Johannesburg. A Memorandum of Agreement between the CSIR and TENET ensures that all institutions that enter into REN Service Agreements with TENET have access to and the use of SANReN.

Under contract to the UbuntuNet Alliance TENET operates UbuntuNet gateways in London and Amsterdam; provides a 10 Gbps interconnection between these two gateways, and provides UbuntuNet with international transit and peering at both gateways. To this end TENET is a member of the London Internet Exchange (LINX).

TENET's Network Operations Centre ("NOC") is located in rented premises on the Main Campus of the University of the Witwatersrand in Johannesburg. The provision of fault reporting and other help desk services at any time of the day or night is outsourced to a larger operator.

5. Subsidiary functions

TENET fulfils three associated subsidiary functions of an operational nature.

First, TENET acts as a Local Internet Registry that manages allocations of IPv4 and IPv6 address ranges within the AfriNIC domain. TENET makes assignments from these ranges for use by campuses that use TENET's Internet services.

Second, TENET is recognised by the ZA Domain Name Authority as the administrator and moderator of the AC.ZA Internet Domain. In this capacity TENET assigns sub-domain names to qualifying institutions, as a public service.

Third, TENET seeks donations to fund capacity development programs. Through the Tides Foundation, Google, Inc made a sizable grant to TENET, which is being used to fund several developmental projects.

6. Looking ahead

Planned backbone extensions: During 2012 Meraka will extend the SANReN backbone to reach remoter towns, including Butterworth, Kimberley, Mafikeng, Makhado, Middelburg, Mthatha, Nelspuit, Polokwane, Potchefstroom, Vanderbijlpark and Welkom.

Rural Campus Connection Project: Also during 2012, using monies made available to HESA by the DHET, rural university campuses will be provided with high-speed connections to the extended SANReN backbone. This is the DHET's Rural Campus Connection Project, for which HESA has appointed TENET as the implementation agent.

Redundant international connectivity: Experience has shown that outages of the SEACOM cable can last for several weeks, and the institutions mandated TENET to secure matching capacity to Europe on another submarine cable, with a view to operating the two circuits as a single protected infrastructure. It is not yet clear whether TENET will execute this mandate or whether the DST and DPE will fulfil the intention that was announced in August 2011 of procuring capacity for use as part of SANReN on the West Africa Cable System (WACS) that is scheduled to be commissioned in June 2012.

SANReN-TENET co-operation: In 2008 the CSIR and TENET executed a formal agreement to collaborate in the deployment and operation of a national research and education network, and to ensure the network's availability to underpin TENET's delivery of research and education networking services to the institutions. The SANReN and TENET teams work well together as regards network planning, design and implementation.

Connectivity within Africa: Telecommunications infrastructures and services are evolving rapidly throughout Africa. TENET will continue support the UbuntuNet Alliance and the development of UbuntuNet's network within Eastern and Southern Africa. In particular, TENET is participating (as a contributor rather than as a beneficiary) with UbuntuNet in the European Commission's AfricaConnect project.

Responsibility for international peering and transit: The time will come when UbuntuNet itself will take contractual and operational responsibility for the peering and transit arrangements in London and Amsterdam and for operating its gateways in these cities.

Development of value-adding services: Ever since its inception TENET's focus has been on the challenge of securing ever more Internet bandwidth for the beneficiary institutions at ever better unit prices. However the substantive deregulation of telecommunications in South Africa[1] means that bandwidth will become a commodity and the unique value that TENET (and SANReN) can offer in future will depend less and less on securing compelling price advantages and rather on the provision of specialised, targeted value-added services that universities and research institutions require. Such services include, for example, the use of very high-speed but temporary, un-routed point-to-point circuits ("light paths") for moving very large datasets to or from anywhere in the World; high quality videoconferencing; and the establishment of so-called trust federations in which many institutions agree to provide each others' staff and students access with access to each others' electronic resources, including but not limited to library and computing resources, using federated authentication and authorisation schemes.

Written by Duncan Martin
Chief Executive Officer

[1] Deregulation of telecommunications in South Africa came not through parliament but through challenges mounted by private industry. In 1996 the then regulator ruled in favour of ISPA against Telkom SA, which had tried to outlaw the emerging Internet Service provider industry by claiming that Internet services were "basic services" that the then Telecommunications Act permitted only Telkom to provide. Effective deregulation of the deployment of infrastructure and the provision of basic electronic communications services occurred in 2008 when ICASA issued I-ECS and I-ECNS licenses to some 400 operators and ISPs, including TENET, following the celebrated court case brought by Altech Autopage Cellular against the then Minister of Communications and ICASA. This allowed infrastructure builders such as SEACOM and Dark Fibre Africa to emerge and allowed TENET and many other operators to own and operate their own optical fibre infrastructures.