FirstNet DATACENTRE SECURITY DOCUMENT

Hosted Services | Connectivity Services | Web Hosting | Voice Services | Cloud Services

Directors A. Sharp, O. Lamusse, V. Gerson (Managing)

Table of Contents

Notice of Confidentiality

All documents are confidential to FirstNet Technology Services (PTY) Ltd. Proprietary information presented in this document may not be used without written consent and remains the property of FirstNet Technology Services (PTY) Ltd unless otherwise agreed to in writing.

1. INTRODUCTION

The purpose of this document is to capture and explain the security policies, procedures and compliance relating to the FirstNet Datacenter. The policies and procedures described in this document have been developed to maintain a secure and safe environment and must be adhered to by individuals performing maintenance or visiting the FirstNet Datacenter. All individuals requesting access to or scheduling maintenance tasks in the Data Centre must understand and agree to these procedures.

2. SCOPE

The scope of this policy covers the following:

- Data centre design specifications
- Information Security Policy
- Data centre physical security
- General Data centre Security policy
- Datacentre access control rules and procedures
- Compliance & Certifications

3. DATA CENTRE DESIGN SPECIFICATIONS

The FirstNet Datacentres are designed in accordance to Tier 2 and Tier 3 International Electrotechnical Commission requirements, comprising of the following:

3.1. Full data-grade HVAC system with redundancy

3.2. Fully redundant air-conditioning units are installed on site. Redundancy includes two units automatically and remotely managed to ensure that any fluctuations in temperature are managed 24/7 and rectified in minutes. Set temperature maintained at 16°C (+/-2 degrees)

3.3. Relative humidity maintained at 45% humidity (+/-5%)

3.4. Redundant Fire Protection- installed by accredited suppliers to SANS code specifications

3.5. Fire proofed doors, and solid walls (2 hours)

3.6. Both smoke and high temperature heat detectors

3.7. Water and Humidity Sensors

3.8. Raised Flooring, structured Cabling.

3.9. All cabling vendors are certified

3.10. All cabling is managed by structured cabling policies

3.11. 24 hour monitoring

3.12. UPS: Dual parallel redundant units ensures a smooth UPS failover during power outages and maintenance windows. Combined with a dual power cable system the Datacentres are extremely fault tolerant.

3.13. Redundant diesel generators

3.2 FirstNet Data centre specification by location

DC 01 Umhlanga KZN Data Centre

Environment
Full data-grade HVAC system with redundancy
Temperature maintained at 16°C (+/-2 degrees)
Relative humidity maintained at 45% humidity (+/-5%)
Redundant Fire Protection
Fire proofed doors, and solid walls
Both smoke and high temperature heat detectors Water and Humidity Sensors Raised Flooring, structured Cabling.
All cabling vendors are certified
All cabling is managed by structured cabling policies

Equipment
85 sqm floor space
19" ventilated racks (600w x 1200d x 42U) All cabinets have unique locks, ensuring that only approved personnel are able to gain access Perforated front and back doors, allows for 86% air flow
Managed Cisco Switch Environment
24 hour monitoring
High Capacity Redundant UPSs Redundant diesel generators (sized to run full load for min of 48 hrs)
Service availability of 99.5% per month

Security
Comprehensive perimeter and building security
Pre-authorisation required for data centre access
Comprehensive audit logs are maintained on all site access
Disk access control at all interior and exterior doors
Biometric access for internal door leading to racks
Digital CCTV surveillance cameras Alarms and early warning messages alert technicians on duty

DC02 Isando, Gauteng Teraco Data Centre

Environment
Multiple cooling zones with independent CRAC units
Temperature maintained between 22°C and 30°C
Relative humidity maintained between 40% -60%
Independent humidity and temperature monitoring in all plenums
Hot aisle containment
Data centre positive pressure to ensure a dust-free environment
Pro-active fire monitoring systems
Diesel generators and tanks are physically separate
All monitoring and fire protection equipment is fed via an independent power source
All cabling vendors are certified
All cabling is managed by structured cabling policies

Equipment
19" ventilated racks (600w x 1200d x 42U) All cabinets have unique locks, ensuring that only approved personnel are able to gain access Perforated front and back doors, allows for 86% air flow
Resilient diesel backup generators are fuelled to provide 5 days of power boosted by guaranteed diesel delivery should the municipal supply fail Fully online UPSs ensure frequency, voltage and surge stability
Power Distribution Unit technology is remotely managed

Security
Comprehensive perimeter and building security
Pre-authorisation required for data centre access
Comprehensive audit logs are maintained on all site access
A visitor's identity is visually confirmed against a picture on a named user list, with additional biometric confirmation through fingerprint imaging Continuous video surveillance of all zones and cabinets Alarms and early warning messages alert technicians on duty
All areas have 24x7 intelligent monitoring and video surveillance with integrated motion sensors A unified building monitoring system logs all security and environment data

DC03 Rondebosch, CT Teraco Data Centre

Environment
Multiple cooling zones with independent CRAC units
Temperature maintained between 22°C and 30°C
Relative humidity maintained between 40% - 60%
Independent humidity and temperature monitoring in all plenums
Hot isle containment

Data centre positive pressure to ensure a dust-free environment
Pro-active fire monitoring systems
Diesel generators and tanks are physically separate
All monitoring and fire protection equipment is fed via an independent power source
All cabling vendors are certified
All cabling is managed by structured cabling policies

Equipment
19" ventilated racks (600w x 1200d x 42U) All cabinets have unique locks, ensuring that only approved personnel are able to gain access Perforated front and back doors, allows for 86% air flow
Resilient diesel backup generators are fuelled to provide 5 days of power boosted by guaranteed diesel delivery should the municipal supply fail Fully online UPSs ensure frequency, voltage and surge stability
Power Distribution Unit technology is remotely managed

Security
Comprehensive perimeter and building security
Pre-authorisation required for data centre access
Comprehensive audit logs are maintained on all site access
A visitor's identity is visually confirmed against a picture on a named user list, with additional biometric confirmation through fingerprint imaging
Continuous video surveillance of all zones and cabinets
Alarms and early warning messages alert technicians on duty
All areas have 24x7 intelligent monitoring and video surveillance with integrated motion sensors A unified building monitoring system logs all security and environment data

4. INFORMATION SECURITY PROCEDURES

4.1. FirstNet caters to the POPI Act regulations by maintaining all client data within the borders of the Republic of South Africa. Physical Data security is maintained via the strict access control procedures described in this document, with a log of all access for records purposes.

4.2. Firewalling is maintained with a focus on segregation of customer data and the security thereof. Best practices are adhered to and penetration testing and auditing assist in helping us achieve this goal.

4.3. Software and Applications are regularly patched and updated to maintain the highest levels of security.

4.4. Electrical equipment is maintained to the highest degree and current is filtered to a single point of entry via Eskom, thus enabling FirstNet to eliminate interference in supply with shared current platforms.

5. DATA CENTRE PHYSICAL SECURITY

The security of customer's business-critical data and systems is our primary concern. To this end, we have multi-layered physical security including comprehensive perimeter and building security, biometrics and video surveillance. Access is controlled to protect both the physical resources and the enterprise data from unauthorized use, accidental or malicious damage and theft.

Entry to each facility is tightly controlled by disc and biometric controls at interior and exterior doors. Strict procedures are in place to monitor and control visitor access both into and within the data center. Preauthorised access to the Data Centers is only granted when a legitimate business need is demonstrated, and comprehensive audit logs are maintained on access. Extensive digital CCTV video camera surveillance is in place throughout the data center areas. Security alarms and early warning alerts get sent to the on duty technicians.

6. DATA CENTRE ACCESS RULES AND PROCEDURES

6.1. Only authorised and documented staff and visitors may enter and perform maintenance within the data center.

6.2. To seek authorisation please contact the Data Centre Manager in the first instance (support@firstnet.co.za) and persons entering the data center must abide by these rules:

6.2.1. Unauthorised persons may not enter the data center

6.2.2. Authorised personnel may not allow entrance to or accompany unauthorized persons

6.2.3. Staff must familiarise themselves with the applicable health and safety rules for working within the FirstNet data center;

6.2.4. Under no circumstances should any customer:

a) Lift floor tiles without prior knowledge, consent, and oversight of the data center manager.
b) Tamper with or interfere with the normal function of the Transformers or Power Distribution Units (PDU).
c) Tamper with or interfere with the normal function of the Air Conditioning units.
d) Plug any device into another cabinet's power supply.
e) Remove any cables or power connections from equipment other than those covered by your SLA.

6.2.5. No food, drink or other 'wet' items (e.g. coats and umbrellas) are allowed into or through the data center.

6.2.6. All packaging and associated materials must be removed from the data center following a visit;

6.2.7. To reduce fire hazards rack enclosures must be kept neat and free of manuals, media, boxes and unused equipment. Rack enclosures are not storage cabinets and must only be used for functioning equipment

6.2.8. Equipment no longer required must be removed as soon as possible after decommissioning;

6.2.9. The appropriate tools must be used for the job

6.2.10. Floor tiles that are moved or removed must be returned in place when completed;

6.2.11. No floor tiles may be left unsettled anywhere in the data center as this can cause obstruction;

6.2.12. Access doors into the data center may not be left unlocked or propped open;

6.2.13. Keys or access tags may not be given to or shared with any other individual

6.2.14. The data center manager must be alerted and informed of any breaches to this security policy.

6.2.15. This Data Center Access Policy may be suspended in the event of an emergency that requires access for medical, fire, or police personnel.

6.3. **Data Centre Access Control**

6.3.1. Access into the buildings, data floors and individual areas is via individually programmed access card

6.3.2. Access into the viewing station and generator rooms is controlled by access tag

6.3.3. Access beyond the viewing station is limited and controlled by Biometrics

6.3.4. Nominated Customer Staff can be given access to perform routine tasks as required

6.3.5. Casual visitors, are not permitted access to the data center beyond the viewing station, except in exceptional circumstances and only with the prior permission.

6.3.6. Standardised procedures ensure that customer's nominated staff can gain access to their equipment whenever required.

6.3.7. Data Centre Access Log - must be maintained at all times by the DC staff. All authorized escorted individuals entering the Data Center must sign the log as they enter and exit for audit purposes.

6.4. **Contractor Access:**

6.4.1. External contractors who require access to the data center in order to undertake maintenance or similar work relating to equipment housed in the data center must notify, where reasonably possible, the Data Centre Manager in advance, and be accompanied by the member of staff responsible for the contractor.

6.4.2. All such visitors should abide by FirstNet's rules for visitors entering the facility, including signingin at Reception and wearing a visitor badge.

6.4.3. Contractors must be made aware of the health and safety and other rules relating to working in the data center.

6.4.4. Contractors requiring access to the Data Centre outside working hours must be accompanied at all times by an authorised staff member of FirstNet.

6.4.5. Deliveries requiring access via the loading bay and external door should be agreed with the data center manager in advance.

6.5. **Periodic Review and Termination of Access**

The Technical Manager will review the access list every 90 days and will remove any individuals who no longer have a legitimate business need to access the Data Centers. The FirstNet Management will review the access list quarterly.

7. DATA CENTRE MAINTENANCE PROCEDURES

7.1. The FirstNet Generators are maintained on a monthly basis with monitoring in place to notify FirstNet Management of all events. Industry specialists are contracted to ensure optimal performance is guaranteed at all times.

7.2. Environmental control is strictly maintained and rotation of dual temperature control units is in place, a strict maintenance schedule is also adhered to and monitored.

7.3. UPS equipment is filtered and maintained with regular checks to ensure all batteries carry sufficient charge in the event of extensive outages.

7.4. Fire suppression systems are maintained on a regular basis with all extinguishers marked and logged with dates of expiry. Datacentre fire suppression is highly monitored and maintained by product specialists.

8. COMPLIANCE AND CERTIFICATIONS

- The FirstNet Data Centre Environment is protected by Fortinet's Fortigate Appliances that are kept up to date and are PCI DSS 3.0 compliant. (Payment Card Industry's Data Security Standards)

- FirstNet is currently in the process of applying for, and is receiving consulting on ISO 9001 (Quality Management) and ISO 27001 (Information Security) certification for the Durban data center. See further details below.

- Our Johannesburg and Cape Town Data centers are co-located in the Teraco data centers (JB1 & CT1) and these data centers are ISO9001 & ISO27001 certified.

ISO 9001 Compliance Status Update June 2015

FirstNet services and products have always been based or build upon best practice, industry standard technologies, methods and equipment. We are ECS and ECNS licensed to provide such services. Even though these technologies and services are individually certified by international and local bodies such as ICASA, we do strive to continually improve our delivery of these products to our customers, and to improve overall customer satisfaction. From its inception in 2012 FirstNet has strived to conform to quality management procedures, involving updating and reworking many of our internal business processes and procedures, measuring the effectiveness of these and updating policy documents accordingly. All legal and contractual documents have come under review, internally and externally.

As part of our Quality Management System, FirstNet has recently embarked on phase two development of a Customer Relationship Management system, which will focus on internal and external workflow and improved customer service deliver and interaction. As some of our services are delivered by authorised 3rd parties (outsourced), the quality management in this regard is also being managed and monitored closely through various levels of interactions with such providers (contractual, technical, service delivery, operational, Executive) and interfaces with our internal systems to provide a seamless services to FirstNet customers.

ISO 27001 – Information Security Management System (ISMS) – Status Update April 2015

As a company that provides hosted services from it Durban, Cape Town and Johannesburg data centres, FirstNet always maintained high standards of security and protection relating to all aspects of its business. As far as compliance and ISO 27001 certification is concerned our Cape Town and Johannesburg data centres are co-located in the already certified Teraco data centres (see attached). Our Durban facility, which is supported and maintained by in-house resources has had security policies and procedures in place from the start, with focus on ultimate asset and data security. FirstNet is in the process of updating and renewing these policies with the aim to become ISO27001 certified.

FirstNet is in the process of receiving consultation on a new ISMS which will address risk assessment methodologies, threat and risk analysis, protection, vulnerability checks and preventative actions.

Notwithstanding the long term investment and projects to formalise the above ISO standards compliances, FirstNet upholds and promotes high standards of security and professionalism. Customer's business-critical data and systems is our primary concern and the FirstNet team is committed to ever improving service delivery and systems that will delight our customers.

Any questions regarding the content of this document may be addressed with Vaughan Gerson, Director of FirstNet.

9. REFERENCE DOCUMENTS

9.1 First Technology group ECNS License

9.2 First Technology Group ECS License

9.3 Teraco ISO 9001 Certificate

9.4 Teraco ISO 27001 Certificate

9.5 FirstNet Fire System Certification

9.6 FirstNet Durban Datacenter Equipment Certification