Republic of Namibia

Ministry of Regional and Local Government, Housing and Rural Development

Tel: (+264 61) 2975111
Fax: (+264 61) 226049

Government Office Park
Luther Street

Private Bag 13289
Windhoek, Namibia

Enquiries: LMJ Heyns
Tel: (+264+61) 297 5069
Fax: (+264+61) 297 5279

Our Ref.: 5/5/16
Your Ref.:

Date: 4 November 2013

Reference number	MRLGH-ICT-P-DRR	**Revision**	1
Title	Disaster Risk Reduction for Information Technology		

	Name	**Designation**	**Signature**	**Date**
Originator	Leon Heyns	Chief Systems Administrator		
Administered By	Leon Heyns	Chief Systems Administrator		
Distribution	Risk Reduction across all segment of Information Technology with the Ministry and Sub-National Government			

Revision History	
Revision 1a	15/03/2013

Contents

Preventive measures General

Definition

Preventive measures are strategies and actions to be taken to protect and safeguard hardware and software against human and natural risks.

Scaled according to requirements

The previous section dealt with the evaluation of each, system's requirements for security. This section both sets minimum requirements for all systems, as requirements, as well as measures to be taken especially to protect sensitive systems (levels 3 & 4.*)*

Minimum Requirements

All systems, terminals and workstations, connected to a system, network or any other communications device will, as a minimum require:

Access Control

- Password control except Public Information Facilities
- Logging of all accesses and updates
- Rigorous exclusions on, and limitation to, user rights
- Facilities located in secure public environment*

Physical Control

- Equipment marked with non-removable identification code *
- If not in a secure area - mechanically secured and enclosed or boxed *
- Network alert for disconnection- or tampering
- Subjected to security system/personnel or police patrol *

Integrity

- Restricted to read only rights, write back of discreet data elements only

(*) These also apply to stand alone systems not network connected.

Maximum Requirements

There is no limit to the degree to which highly sensitive or valuable information may be protected. The analysis of system sensitivity will define the level of requirement for a given secure environment. A typically secure environment will include full protection for the risks described in the designated pages which follow.

Preventative measures - Human Factors

The following risks can be substantially reduced by implementing the recommended practices described below:

1. Unauthorized access or attack on protectively marked and sensitive information, assets and people.
    - Logging of accesses and updates
    - Access control lists
    - Authentication of users
    - Protection, of passwords
    - Ensuring that the location of computer facilities is not public knowledge by baring access by any news media personnel
    - The vetting of employees through security checks
    - BIOS level passwords and automatic sign-off of inactive stations

2. Spying and/or disclosure of information by authorized personnel with, access or proximity to sensitive and protectively marked information.
    - Logging of accesses and updates
    - Have a sign-in station
    - Use a lock screen when interrupted while dealing with sensitive information.

3. The acts of intrusion and violence.
    - Use of coded or combination locks, smart cards, security keys
    - Locate room away from normal traffic flow
    - Entrance to building must be securely locked
    - Kicking, slapping- and sabotaging terminals must be heavily punished

4. Damage to equipment and loss of data as a result of inadequate power, falling objects, fire, floods etc.
    - There must be constant and even electric flow to the equipment as well as a standby power system (Uninterruptible power supplies (UPS)) must be provided for key servers
    - Proper roofing to prevent water leakage
    - Deploying appropriate fire and smoke detectors, water detection, etc.
    - No eating, drinking and smoking in the computer room

5. Theft by employees or outsiders
    - the use of guards and video cameras around the computer room
    - lock rooms when not in use
    - use of burglar alarms
    - use of coded or combination locks, smart cards, security keys
    - restrict entry to the computer environment
    - Comprehensive security system monitoring all access.

6. Access of unauthorized entities into the operating system, utility
    - Programs, application programs and data.
    - Eavesdropping protection (encryption of classified information to prevent eavesdropping
    - Impersonation over electronic channels must be prevented by a longer term strategy to adopt digital signatures and electronic authentication for use in electronic communication, ail other communication media must use official correspondence material and be in writing or duly signed (written form).
    - Worms and virus protection software must be installed in all servers, desktop computers and terminals.

7. Tapping of communication media
    - Wherever possible cables must be protected and for all sensitive systems data encryption must be used end to end or within link layers to ensure transmissions remain secure
    - Armoured conduit must be installed for exceptionally sensitive systems
    - Where possible power and communication lines must be underground

- Cables must not be routed through, public areas to minimize physical access to them
- use of anti-theft cabling system
- checking of physical lines

8. Contaminating data, operating systems, utility and application programs
    - Users must never give their usernames and passwords to others

Preventative Measures - Natural Factors

Natural/Environmental risks

Hardware and software can be protected from natural disasters as follows:-

a) Power Spikes, Fluctuations or Failure
   - Install uninterrupted power systems
   - Install separate and clean power lines

b) Lightning
   - Install lightning prevention appliances

c) Extreme temperature and humidity
   - Apply air conditioning

d) High Levels of Static Electricity
   - Treat carpets and surfaces with anti-static solution
   - Install anti-static mats in front of sensitive equipment

e) Dust
   - Doors and windows to be closed to minimize dust pollution
   - Hardware components must be cleaned regularly with antistatic liquids

f) Earthquake and floods
   - Keep backup copies away in a different building
   - Keep windows closed when it is raining or when rain is expected
   - Locate computer rooms far away from storm water pipes or run off

g) Fire
   - Have smoke detectors and fire extinguisher installed

Preventative Measures - Safeguarding

Safeguarding Sensitive Systems in a secure area

The following safeguard measures must be applied:

a) All sensitive computer hardware, software and data must be installed, operated and stored within a security area.
b) All areas where sensitive computer related equipment and data is used must be guarded 24 hours a day. Guards must have knowledge of all security procedures and be in continuous contact with a duty - control room.
c) No unauthorized persons may have access to the security area.
d) In terms of policy, comprehensive insurance must be taken out to cover all equipment and human aspects in the event of disaster
e) Computer vulnerable points. Because of the composition and working of computer systems, certain critical facilities exist which require special safeguarding. Those vulnerable points in the computer environment are as follows:

Computer Hardware

a) Centralised computer systems and network servers
b) Any computer connected to a communications device of any kind
c) Peripheral devices (terminals, printers, modems, fax-modems etc.) which are not under individual control or in a secure area when not in use
d) Computer terminals and Workstations not under individual control or secure area when not in use.

Computer Software

a) Network Operating Systems
b) Name and List Server Systems
c) Data encryption utilities and source code
d) Software Applications and related data

Supporting Hardware

a) Power and Uninterrupted Power Systems
b) Data communication networks

Supporting Infrastructure

a) Air-conditioning equipment
b) Fire fighting equipment (Fire detectors, -extinguishers and -alarm equipment)
c) Access control equipment
d) Power surge(spikes)protection and lightning protective devices

These vulnerable points must be placed within a closed or restricted area.

The safeguarding measures in respect of the above mentioned vulnerable Measures points as to comply with the following minimum security requirements:

The Computer

- Hardware must be kept and used in a closed area.

Peripherals

- This equipment must at least be kept and used in a restricted area. The users of this hardware will usually be placed in a closed area.

Air-conditioning Equipment

- Both, central and free standing air-condition equipment installed specifically or computer equipment must at least be placed in a low security area.
- Vents must be located to ensure a clean air supply. Unauthorized persons must not be able to reach, or be able to stop, or tamper with air-condition equipment.

Electricity Source

- Each user is responsible for the safeguarding of power cables within the security area and must ensure that unauthorized persons cannot interrupt power supply or be able to cause a large fluctuation of the power supply. Where a generator is used to produce electricity for computer related equipment, such equipment must be installed in a restricted area and be safeguarded.

Uninterrupted Power Supply UPS) and Emergency Power Source

- This equipment must at least be installed, and used in a restricted area. File Servers, Communications Equipment and Ventilation must, at least, be able to be supported for the shutdown period by this power supply. Any emergency power source must also be installed within a restricted area.

Data Communication Network

- All network equipment like control units, modems, nodes, etc. with the exception of cables must be used and installed in a restricted area. Other Network systems shared by Defence Force and the general public must not be interfaced with the exclusive Defence 'Network systems. All cables not under the jurisdiction of Namibia Post and Telecom, must comply with the same security requirements as power cables.

Firefighting Equipment

- Fire fighting equipment must be installed in. all security areas where computer related equipment are used or are being installed. This equipment must be placed in such a way and be inspected regularly that it will always be available and ready in case of emergency.

Fire sensors/Alarm systems

- In cases where fire sensors cause a false alarm, it must be immediately investigated and repaired or replaced. Care must be taken that all automatic fire fighting systems are activated when the building/area is vacated. Fire and evacuation procedures must be prominently displayed and a fire drill is to be conducted at least once per year.

Access control equipment

- The equipment which control access by personnel must be safeguarded so that unauthorized access cannot be achieved by sabotaging this equipment or be achieved in an emergency situation. Alternate access control measures must be available.

Preventative Measures - Control of Personnel

Control of Personnel Movement

Access control and movement of personnel in areas where computers and computer related equipment are installed and used, is one of the most important precautions which must be adopted.

Access control must be of such a nature that:

a) No unauthorized person can have access to a security area.
b) All personnel can be positively identified
c) At any time it can be determined what access rights (or level of access) a person has, or can be granted, within the area concerned.
d) While in a security area, visitors or contract workers not in possession of a security clearance must at all times be under supervision of a security officer or an official of the division concerned. In case of contract workers it must be determined and confirmed that authorization has been given to deliver the service.
e) Vehicles not property searched must not be allowed in any security area.

Transportation Control of Computer related articles

For the proper protection of computer related articles in transit it is necessary that:

a) A permit system must exist for the removal of computer related articles from a security area. Permits must be controlled by the security staff of the facility concerned.
b) Computer related articles may not be left unguarded outside a security area.
c) Necessary precautions must be taken to assure that computer related articles are not destroyed or exposed to sabotage during transportation.
d) Care must be taken that computer related articles are packed properly to prevent damage or unauthorized access.
e) Computer related equipment must on arrival at their destination be handed over to authorized personnel. The receiver of computer related articles must acknowledge receipt of delivery by signature. The Register of signatures is to be controlled by security staff of the instance concerned.
f) When dispatching electronic storage media of a valuable or confidential nature (e.g. floppy discs, magnetic tapes, CDs etc.) or system backup media an escort must be provided

Preventative measures - Personnel Security

Measures regarding Personnel Security

These security measures are taken in respect of sensitive systems and/or information to ensure that:

a) Personnel do not commit, or are not tempted to commit, sabotage, espionage or subversion.
b) Personnel are not exposed to the risks of subversion and/or espionage.

Actual Personnel Measures

a) All computer users must be formally trained; the training must include computer security, before access to the computer may be allowed.
b) It is the responsibility of authorized personnel to assure that computer related articles, like computer printouts, etc. do not come within reach of unauthorized persons.
c) Security clearance. To be able to execute personnel security, all personnel working with, computer related equipment data or personnel must be security cleared. The minimum security clearance to be obtained is a. "Super Confidential clearance". The security classification of the data, with which the employee will work, determines the clearance of personnel to "Secret" or "Top Secret".
d) Systems administrators Responsibility- Systems administrators at all levels are responsible to ascertain that the security grade (or classification) of the data to which access is given or obtained does not:
    - Exceed the security clearance of the staff member or
    - Any upgrading does not exceed the staff member's current post.
    - The operator concerned has signed an undertaking as per appendix A to this directive.
e) A high standard of security awareness must be maintained by means of training, information, exercises, drills and by conducting computer security refresher courses.
f) Security breaches or threatening behaviour must be reported to the security staff without delay.
g) Failure, on the part of systems administrators, or supervisors to follow these instructions will be considered in a serious light and offenders will be charged with misconduct in terms of section 25 of the Public Service Act No. 13 of 1995.

Preventative Measures - Software Security

Definition Software Security

Software Security is the protection of data and programs in a computer system.
Security of Data and information is one of the most important aspects of computer security.

Background to Software Security

- People can break into a computer to retrieve, change or destroy data.
- Every attempt must be made to prevent unauthorized access and to protect computers from harm.
- Access must be controlled by a matrix that grants authorization to view or change specific data and information
- Confidential data must be highly protected so that a user does not "fall into" a file accidentally.
- All essential programs, software systems, data and associated documentation must be kept under lock and key.
- This information (including software and data) must also be backed up with extra, copies kept in a. separate location, so that operations can quickly resume in an event of disruption, or disaster.

Aims of Software Security

The aims of software security are to protect the following:
Source programs, object programs, utility programs, communication programs, and diagnostic including operating systems.

Potential Risks

- Unauthorized access
- Destruction, change, copying of data or programs
- Spying on data or information

Preventative Measures - Network Security

Software Protection Measures

a) Determination of access control of each user
   - Access control is the regulation that is put in place on how users gain access to an account, what files they can change, read or execute and what resources they can use.

b) Users rights must be specified in writing and the record retained
   - MRLGHRD must determine who gets an account. A supervisor must fill out a form which spells out a user's permissions. The form is then given to the system administrator who issues the account.

c) Users must commit to standards in writing
   - All users must sign a that they have read, understood and accepted the security policies of the government which, Inter alia, includes the following conditions and consequences to which they have agreed,

They <u>will</u> not:

d) Attempt to break, into another user's accounts or try to crack passwords for this purpose,
e) Access, or attempt to access programs or data, other than that which relates to their responsibilities.
f) Modify files (or data) which they are not authorized to operate on.
g) Share accounts or reveal, their passwords to anyone at all
h) Introduce unlicensed software onto the network or any workstation.
i) Knowingly use software which, is unlicensed
j) Use the network: to access or attempt to access sites or hosts which they are not authorized to access.
k) Propagate chain-Letters or conduct mail-bombing (spamming) from the network
l) Knowingly introduce viruses, worms or Trojan horse software onto the network

Any person making himself herself guilty of any one of these offences will automatically be construed to be in violation of government security and will, as such, be charged with misconduct

Software protection Methods

In turn, they will:

a) Have a responsibility to assist in the protection of the systems which they use (e.g. by following disk virus scanning procedures, reporting possible security weaknesses or violations and situations which could have security risks.
b) Adhere to generally accepted 'netiquette' when interacting on the Internet, should such access be granted.
c) Only use the computer systems and networks made available to them for the legitimate work of the government or for investigation/s which will have consequential benefits for the effectiveness and efficiency of government

Failure to implement the above will be construed to be negligence of government security and will, as such, receive a written, disciplinary warning.

Password Management

The most basic security measure is the password. The weak link in password-based security is the user. The following must be implemented

- Passwords must be unique and have no relationship to information connected to the user; his family, relatives or friends.
- Passwords must be sufficiently long, complex and used for a short duration as that they are extremely difficult to crack.
- Passwords must be kept confidential, known and used by only one person.
- Each password must be unique and unrecognizable in relation to any password used in the past or by another computer user.
- Under no circumstances must a password be given to another person.
- A login which has taken place via a particular password will always be considered to have been effected by the user to whom the password legitimately belongs.
- Logins must not remain active for longer than 5 minutes without being activated
- Nobody must leave a password laying somewhere/ where it is visible or accessible.

Giving one's password to another person is the same as giving them the keys to a classified government building and contraventions will be viewed in that light since this can potentially compromise government security.

See Appendix B
Additional information on password security can be found in this appendix. The implementation and/or extension to these guidelines will be the responsibility of each respective Ministry.

Account Policy restrictions

- Maximum number of bad Logon attempts is 5 Restrictions
- Log on hours (to be determined by MRLGHRD)
- Grace logins after password has expired is 1
- There must be account auditing for each user
- Accounts of people who have left the Ministry / Offices must be removed
- A user's task change, or change in rights must be reflected on the account
- Re-evaluation of users' security permission must be carried out by the supervisor
- All user accounts must have expiry dates of 3 months

Auditing Policy

Auditing is the process of tracking selected, users and activities and storing Data in a security log. This process can be used to identify unauthorized access to resources and/or programs. Therefore, the following points must be enforced.

- Monitor successful and unsuccessful logins
- Monitor resource and file access

Securing Servers/Desktop/Workstation

- All computer users must log out from the network whenever they finish using the computer or if they go out of the room
- They must frequently check all systems for the presence of viruses.
- Ensure that all incoming software/ data, is checked for the presence of viruses

Securing a network against network data packet snooping

- Use public/private key encryption method for sensitive or confidential information
- Before new software / data are introduced to the system, it must be scanned for viruses. MRLGHRD must have a number of people who have write access and these people must be instructed on how to safely load new software.
- Dial-up access must be limited to less sensitive information such as e-mail, Internet, but not information. that can be harmful if intercepted
- MRLGHRD must identify a set of key words which will identify information which is either not required or undesirable via the Internet; this together with undesirable site addresses (TJRLs) will be used to block access.
- Discourage computer use for private matters (theft of computer time).
- Ensure the use of unique usernames
- Packet filtering: All incoming' packets will be scrutinized and only recognized and selected packets will be allowed to enter into the GRN Intranet.
- A combination, of Proxy server or Firewall and DNS server, will be used to prevent access by unauthorized people from outside the Intranet. Only selected access will be allowed through the proxy and firewall. IP addresses from outside the intranet will be translated into our own network addresses and forwarded to their Internal destination
- All workstations and servers which, are attached or given access to the Internet or any other public access system will have virus scanning software installed
- All copies of virus protection software will be kept up to date, new releases are to be installed within 5 working days of receipt.
- No browser enhancements, add ins, or other public network, utilities (FTP software, News or Mail readers, multimedia plug-ins, Telnet capabilities etc.) will be permitted except those which have been officially approved by the Directorate of Information Technology Services - Management
- Loading code cracking or decryption software, on any workstation or server, which could compromise or prejudice the computer system security of the government or potentially make information available to someone who is not authorized to access or view it, will constitute a dismissible offence.
- The use of software for which written authorization cannot be produced will, in all cases, constitute an infringement which will be subject to the formal disciplinary procedure.

Information and Data Security

Definition

Data Security entails those security measures to be taken, ensuring that data, computer related or not, will not be subject to sabotage or espionage.

Preventative Measures

Over and above the physical - and personnel precautions, the preventive measures mentioned below must be implemented to ensure data security:

Security Classification

The classification, control and distribution of computer related articles and printouts must be handled in the same manner as documents according the classification thereof as prescribed in the PSCOIT security prescriptions.

Allotment of Security classification

A security classification must be allotted to all computer related articles/printouts. The minimum classification for any article/printout must be "RESTRICTED''. The system owner will determine the classification, according to the date on/in the article/printout.

User Need Specification

The security classification must be determined by the user and the project: managers of the Ministry. The necessary measures for ensuring data security must also be explained- Those measures must be approved by die Chief of the Ministry intelligence

Handling

The security classification of data must be indicated clearly and readable in all cases of data in physical form, for example: printouts, manuals, lists, magnetic tapes, discs etc. These must be stored according to their security classification.

Note on Deletions

The deletion of a file does not remove its contents from a magnetic drive or Disk. In most cases it can be restored. System administrators must ensure that deleted files are thoroughly removed (or wiped) from any disk on a regular basis.

Backup Routines

All computer equipment is subject to failure at some time. The presence or absence of a backup of all software (operating systems, source code, applications and data) can mean the difference between almost immediate recovery and long term disaster. It is the system administrator's direct responsibility to ensure that backup procedures are established, implemented and regularly tested for reliability.

How many backups?

A single backup will frequently fail unless it is stored on a virtually indestructible medium like a CD-ROM, which, has also been tested for integrity and reliability. Magnetic storage mediums are considerably less stable and their stability tends to reduce as the medium ages. Three backups on a magnetic medium must be considered the minimum. In the case of a RAID or set of mirrored, disks this can be reduced to no less than two.

Factors to be considered in terms of both the number of backups retained and the frequency with which backups are created are:

- The frequency with which the information changes
- The speed with which errors in the data will be identified
- The volume of the changes to data, which take place
- The degree of difficulty experienced in recreating new records and/or changes
- The actual cost of recreating and/or updating the data if not recovered
- How critical the computer system is in both financial and operational terms

Minimum Backups

The minimum backup method will include three generations of all data which are continually maintained.
This is described as the grandfather, father and son arrangement.

Testing of Backup Procedures

Any backup procedure must be tested on a regular basis. Actual backups must be examined for integrity and reliability. The full backup must be restored to a separate disk drive and the full functionality of all applications and their related data thoroughly tested.

Storage of Backups

Backups must always be stored, in dry, insulated, fireproof and secure cabinets in a separate building which has at least the same level of security as the system from which the backups originated.

Computer Access Control System

Accessing and storing Sensitive Data

If sensitive computer related data is to be stored, such data must be protected by means of a "Computer Access Control System". The access control system is a pre-requisite when implementing any system working with classified data. The creation of such access control system must be done by the Ministry's Information Systems Division. The access control system must provide for the following:

a) The positive identification of users.
b) Identification of data to which the user can have access.
c) Identification of the terminal from where the user can have access.
d) Access authorization to the data, if the user is authorized and security cleared, and refusal of access to unauthorized/security restricted persons.
e) The logging and storing of activities on the system, to determine at a later stage who, what, when and where activity took place.
f) Any operator for any specific system must be registered for these rights by the system, manager who is also responsible to ensure that the periodical change of passwords takes place.

Access to data Regulated

- System managers are to ensure that access to data by all users, within the Ministry concerned, is in direct relation to the user's security classification. They must also ensure that all applications for access to the system are done in the prescribed manner.
- Access to computer related articles must be strictly controlled. Only authorized persons can have access. A register system must be used to control the flow of articles. The removal of computer related articles must take place against signature.

Minimum Access Granted

Each user must have minimum computer related access to enable him/her to effectively execute his/her allotted task.

Data-loss prevention

Step 1.

Determine where the primary point of data control should be—at the endpoint, the network, or a combination of both. There are many different approaches to data protection, from network-level data-loss prevention suites to laptop encryption technologies and everything in between. To decide what's best for your business, begin by determining where the primary point of data control should be.

Endpoint technologies protect intellectual property from theft or unauthorized dissemination, such as preventing someone from downloading a customer list onto a USB drive and walking out the front door. The value of network solutions lie in monitoring how information is used within the organization so you can identify and correct faulty business processes. Some small businesses begin with a data discovery project simply to understand where their sensitive data exists and determine their level of risk.

Step 2.

Selecting the right data-security solution begins with research. Take advantage of readily available research in published analyst reports to understand product capabilities. Look for a solution that provides the flexibility to take an incremental approach and provides coverage across a broad array of communication channels including e-mail, Web traffic, instant messaging, peer-to-peer, streaming media, and endpoints such as USB drives, printers, desktops, and laptops.

Some small businesses will opt for a data-loss prevention solution that spans the network and endpoints. Others will find value in e-mail security solutions that monitor outgoing e-mail for sensitive information. Still others will opt for endpoint encryption technologies.
The important point is that more small businesses must begin enforcing data-security policies. A single data breach can have lasting repercussions. With the right policies, technology, and employee education, you can mitigate your risk.

DRAFT Service Level Agreement Template

SERVICE Level agreements for maintenance and uptime.

Title:	**Service level agreeement** between **Client** and **service provider**
Description:	This document is a Service Level Agreement (SLA) between <Client> and **<Service Provider>**, outlining the responsibilities and level of service that will be provided.
Date:	DD MM YY
Effective Date:	DD MM YY

Distribution List

Name	Role	Company	Info/Sign Off

Table of Contents

1 Executive Summary

This document is a Service Level Agreement ("SLA") which defines the service agreement between (<CLIENT>) and <Service Provider>. <Insert key aspects of service and reason for agreement>

This agreement outlines the facilitation of the services to <CLIENT> by <Service Provider>, along with the relevant responsibilities and expectations necessary to enable the required services.

All service areas will be discussed during monthly review meetings between <CLIENT> and <Service Provider>. The objectives of these meetings are to assure that each service area is relevant, that satisfactory service levels are reached and to ensure that the responsibilities have been fulfilled by both parties.

The service definition will be formally reviewed on an annual basis and this agreement will be updated accordingly.

Amendments to the contents of this agreement are made by the mutual agreement of <CLIENT> and <Service Provider>. The Document will be maintained by <CLIENT> and will remain valid until a revised agreement has been mutually endorsed by both parties.

1.1 Purpose and Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent service support and delivery to <CLIENT> by <Service Provider>.

The **goal** of this Agreement is to obtain mutual agreement for service provision between the <Service Provider> and <CLIENT>.

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to <CLIENT>.
- Match perceptions of expected service provision with actual service support & delivery.

2 Roles, Responsibilities and Service Commitments

2.1 Contacts

The Account Manager from each party will maintain responsibility for the relationship on their respective sides of the agreement. The following are the Authorised Persons from each party:

2.1.1 <Service Provider>

Name	Role	Phone	Email
	SLA Account Manager		
	Analyst		
	Analyst		

2.1.2 <CLIENT>

Name	Role	Phone	Email
	Service Owner		
	SLA Manager		
	Analyst		
	Analyst		
	Analyst		
	Analyst		

2.2 Responsibilities

The Account Manager within <Service Provider> will have responsibility for the performance of <Service Provider>'s activities outlined in this agreement, along with the appropriate risk management activities.

<insert any other relevant responsibilities>

2.3 Effective Date

This Agreement is valid from DD MM YYYY

2.4 Duration of the Agreement

This Agreement shall remain in place for an initial period of X years from the commencement date, and thereafter shall renew for a period of X year, subject to annual reviews. <CLIENT> have the power to terminate the agreement at any time within good reason. If this occurs <CLIENT> retains rights and ownership over all <CLIENT> related documentation, information and files.
Support Structure

2.5 People and operating hours

<Service Provider> will provide <CLIENT> with various support features, as listed below:

- <insert as appropriate>

Support Personnel

<Service Provider> will provide competent personnel with the necessary skills and experience to provide the support services. <Service Provider> will use its sole discretion in selection of all its personnel nominated to carry out the services. If however, in <CLIENT>'s reasonable opinion, any of <Service Provider>'s personnel fail to carry out the services with sufficient competency, <CLIENT> may notify <Service Provider>. Upon such notice, <Service Provider> shall rectify the situation as soon as is reasonably possible. (suggested wording only!)

2.6 Key Personnel Changes

To allow for continuity of service both parties must inform each other of significant departures or changes in the responsibilities.

Service Element	RESPONSIBILITIES <Service Provider>	RESPONSIBILITIES <CLIENT>
Personnel Change Notification	• <Service Provider> will notify <CLIENT> of any changes in personnel roles within X weeks of change date • <Service Provider> will notify <CLIENT> of any changes in personnel responsibilities within X weeks of change date	• <CLIENT> will notify <Service Provider> of any changes in personnel roles within X weeks of change date • <CLIENT> will notify <Service Provider> of any changes in personnel responsibilities within X weeks of change date

2.7 Place of Service Delivery

<Service Provider>

Street Name
Street District
City
Region

2.8 Issue Management

<Service Provider> will immediately notify the <CLIENT> Account Manager of any material developments that will have an impact on the ability of <Service Provider> to carry out the services effectively. This also applies to developments that will have an impact on the compliance of the service with the applicable laws and regulatory requirements.

<Service Provider> will log and keep track of all developments and any issues raised by <CLIENT>. All open issues will be discussed at the monthly partnership review meetings.

2.9 Disaster Recovery / Business Continuity

<Service Provider> has effective Disaster Recovery / Business Continuity plans that are tested on a regular basis

<insert details>

3 Service Definition

The following sections detail the services and associated responsibilities pertaining to this agreement. All metrics will be consolidated and reviewed on a weekly/monthly/quarterly/annual basis

<insert all services below as per table.

Service Line	Service Level Name	Total Description	Measurement Description	Target Level	Green Level	Amber Level	Risk Level

All metrics should be reported on at agreed intervals.

4 Signatures

<CLIENT>

Name	Role	Date	Signature

<Service Provider>

Name	Role	Date	Signature