RED STAR EXPRESS PLC. IS POLICY AND PROCEDURE MANUAL

INTRODUCTION AND TERMS

The IS policy and procedure manual is that which guides and give directions to the general operations of all IS staff and users of the IS infrastructure at large. This Manual belongs to IS Department Red Star express Plc. and does conform to and compliments the company's policy as a whole.

The IS Policies and Procedures in this handbook are binding on all staff of Red Star Express Plc. and Subsidiaries. It is expected that staff read, understand and adhere to the policy and procedure stated herein. After reading, if there are any misunderstandings or disagreements to which a staff cannot adhere to certain policies, such should make it know in writing to the IS manager and HR respectively.

THE UNIT OBJECTIVES

- ✓ To provide Information Systems platforms to all units in the Company and ensure their smooth operation.
- ✓ To provide technical support to the users of the Information Systems platforms within the company.
- ✓ To ensure safety of all IS infrastructure and gadgets as the case may be.
- ✓ To ensure the safety of all company's data financials and non-financials by ensuring a proper system back up and checks

UNIT STRATEGIES

The IS unit will ensure that;

- ✓ All IS infrastructures (Computers, Printers, Servers and Scanners etc.) are properly maintained and serviced quarterly.
- ✓ All developed in-house and off the shelf programs are running effectively at all times.
- ✓ All network servers are up and running optimally at all times, minimizing downtimes to the barest minimum by ensuring proper monitoring.
- ✓ Internet Connectivity and Company website will be properly maintained to ensure they are up and running effectively at all times and minimize downtime
- ✓ Request for computer equipment and services will be promptly handled with necessary approvals in place
- ✓ Responses and resolutions of incidences reported are promptly treated.

UNIT FOCUS

The Unit will;

- ✓ Strive to keep abreast with current technology and deploy same to achieve higher productivity.
- ✓ Ensure a virus-free network is maintained at all times.
- ✓ Be proactive in its approach to ensure the smooth running of our computing equipment.

Policy

PURPOSE

The purpose of this policy is to provide direction and guidance through the establishment of minimum information technology procedure standards for use within IS Dept. of Red Star express Plc**.** and for other units within the organization which might require any form of IS service.

- ✓ To establish a Red Star express Plc. -wide approach to information security.
- ✓ To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of Red Star express Plc. data, applications, networks and computer systems.
- ✓ To define mechanisms that protects the reputation of the Red Star express Plc. and allow the Red Star express Plc. to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- ✓ To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

POLICY BENEFIT

The main benefits to having this policy and procedure manual are as follows;

- Ensures all staff are aware of obligations in relation to selection, use and safety when utilising information technology within the business
- It's a proven way to help managers and supervisors make consistent and reliable decisions
- Helps give each employee a clear understanding as to what you expect and allow.
- It might take a little effort to complete and compile, but brings definite long-term benefits, reduces disputes, and adds to the professionalism of our business.

SCOPE

The following procedures provide an integrated holistic approach to security

USER ACCOUNTS MANAGEMENT

Access to computer systems is controlled by usernames and passwords. All users will be provided with a user account and password.

User accounts will be limited to one account per user or staff member. A written memo/Email from HR is required to open accounts for new staff.

METHOD

An authorized user account request form from Dept./Unit head to the information technology Dept. is mandatory for all staff. User accounts will be created / deleted in any application based on the details entailed in a request form.

- All user access to the core system applications will be uniquely identified through the use of user account
- Access to functional procedures within the application will be provided on the basis of grouped/sectional functions determined in conjunction with the Unit/departmental heads to ensure appropriate segregation of duties.
- Changes to the user account profiles in any application will be controlled by the Unit Head.
- Changes to the user account functions will be made on receipt of an authorized request form.
- A list of user accounts and their functional access levels will be provided to the business owners for approval.
- All software resident on a server shall be documented.
- Staff user accounts will also be disabled /deleted based on a termination report sent from Human Resources Unit.
- Head of Units can request that user accounts be manually altered if necessary

INFORMATION SECURITY PHYSICAL AND ENVIRONMENTAL POLICY – Password Management; IS Physical and Environmental Security

PURPOSE

Red Star Express Plc. will provide value added logistics solutions that will be secure, prompt and effective through: PEOPLE, SERVICE & PROFIT. This policy establishes the Enterprise Physical and Environmental Protection Policy, for mitigating the risks from physical security and environmental threats through the establishment of an effective physical security and environmental controls program. The physical security and environmental controls program helps Red Star Express Plc. protect its Information Technology Assets from Physical and Environmental threats.

SCOPE

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by Red Star Express Plc. Any information, not specifically identified as the property of other parties, that is transmitted or stored on Red Star Express Plc. IT resources (including e-mail, messages and files) is the property of Red Star Express Plc. All users (Red Star Express Plc. employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

INTENT

The Red Star Express Plc. Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish minimum standards for the physical and environmental protection of Information System assets.

POLICY

Red Star Express Plc. has chosen to adopt the Physical and Environmental Protection principles established in the private policy **CODE**s of "Physical and Environmental Protection," Control Company **CODE**s, as the official policy for this domain. The following subsections outline the incident management standards that constitute Red Star Express Plc. policy. Each Red Star Express Plc. Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related to the standards documented.

CODE-1 Physical and Environmental Protection Procedures: All Red Star Express Plc. Business Systems must develop, adopt or adhere to a formal, documented physical and environmental protection procedure that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

CODE-2 Physical Access Authorizations: All Red Star Express Plc. Business Systems must develop and maintain a list of personnel with authorized access to the facility where the information assets reside (except for those areas within the facility officially designated as publicly accessible). In addition, documentation must be retained to capture the authorization and provisioning of physical access to all Red Star Express Plc. Business System facilities. Also, a periodic physical access review and approval process must be implemented to validate the appropriateness of physical access at these locations.

CODE-3 Physical Access Control: All Red Star Express Plc. Business Systems must enforce physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information asset resides (excluding those areas within the facility officially designated as publicly accessible). This includes:

- Validate individual access authorizations before granting access to the facility.
- Control entry to the facility containing the information asset using physical access devices and/or guards.
- Control access to areas officially designated as publicly accessible in accordance with the Organization's assessment of risk.
- Secure keys, combinations, and other physical access devices.
- Inventory physical access devices on an annual basis.

- Change combinations and keys at least annually when keys are lost, or individuals are transferred or terminated as combinations could be compromised.

CODE-4 Access Control for Transmission Medium: Not in Scope.

CODE-5 Access Control for Display Medium: All Red Star Express Plc. Business Systems must restrIS and control physical access to information asset output devices to prevent unauthorized individuals from obtaining the output.

CODE-6 Monitoring Physical Access: All Red Star Express Plc. Business Systems must monitor physical access to the information asset to detect and respond to physical security incidents. This includes review of physical access logs every 30 days and coordinates the results of the reviews with the organization's incident response capability.

CODE-7 Visitor Control: All Red Star Express Plc. Business Systems must restrIS and control physical access to the information asset by authenticating visitors before authorizing access to the facility where the information asset resides other than areas designated as publicly accessible.

CODE-8 Power Equipment and Power Cabling: All Red Star Express Plc. Business Systems must protect power equipment and power cabling for the information asset from damage and destruction.

CODE-9 Emergency Shutoff: All Red Star Express Plc. Business Systems must be able to shut off power to the information asset or individual asset components in emergency situations. In addition, emergency shutoff switches or devices must be placed in clear and accessible areas to facilitate safe and easy access for personnel.

CODE-10 Emergency Power: All Red Star Express Plc. Business Systems must provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information asset in the event of a primary power source loss

CODE-11 Fire Protection: All Red Star Express Plc. Business Systems must employ and maintain fire suppression and detection devices/systems for the information asset that are supported by an independent energy source.

CODE-12 Water Damage Protection: All Red Star Express Plc. Business Systems must protect the information asset from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

CODE-1 Delivery and Removal: All Red Star Express Plc. Business Systems must authorize, monitor, and control shipments and equipment removals from the facility and maintain records of those items.

CODE-15 Alternate Work Site: All Red Star Express Plc. Business Systems must employ IT controls, such as logical and physical access controls, at alternate work sites as applicable.

CODE-18 Location of Information Asset Components: All Red Star Express Plc. Business Systems must position information asset components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

INFORMATION SECURITY-PASSWORD MANAGEMENT

INTRODUCTION

A **password policy** is a set of **rules** designed to enhance computer security by encouraging users to employ strong **passwords** and use them properly. A **password policy** is often part of an organization's official regulations and may be taught as part of security awareness training.

OVERVIEW

Passwords are an important aspect of computer and data security. A poorly chosen password may result in unauthorized access and/or exploitation of Red Star resources. All users, including contractors and vendors with access to Red Star systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

PURPOSE

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

SCOPE

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Red Star Express (RSE) facility, has access to the Red Star Express network, or stores any non-public RSE information.

POLICY

Password Creation

- All user-level and system-level passwords must conform to the Password Construction Guidelines.
- Users must not use the same password for RSE accounts as for other non- RSE access
- Where possible, users must not use the same password for various RSE access needs. E.g. (using same password for Windows and RSE Application)

Password Change

- All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis (30-60Days)
- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every 30-60days
- Password cracking or guessing may be performed on a periodic or random basis by the IS Team. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential RSE information.
- Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share RSE passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

- Do not use the "Remember Password" feature of applications (for example, web browsers)
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Application Development

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.
- Applications must provide for some sort of role management; such that one user can take over the functions of another without having to know the other's password.

COMPLIANCE MEASUREMENT

The RSE IS team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions: Any exception to the policy must be approved by the IS department in advance.

Non-Compliance: An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. All password management by employees as long as it relates to working with Red Star Express must comply with the policy herein

INFORMATION SECURITY- IS PHYSICAL & ENVIRONMENTAL SECURITY

INTRODUCTION

All RSE IS facilities supporting critical or sensitive business activities should be housed in secure areas. These facilities should be physically protected from unauthorised access, damage and interference. They should be located in secure areas, protected by a defined security perimeter, with appropriate entry controls and where appropriate security barriers. As

information accessibility is essential to business, RSE is committed to providing effective IS facilities physical environment conditions and security to safeguard equipment and information from unauthorised intrusion and damage and, to provide optimum equipment operating performance. The planning and implementation of IS equipment environments, security safeguards and controls, procedural, access control, architectural, electrical and structural requirements is essential.

PURPOSE

In respect to this policy the term physical and environmental security refers to controls taken to protect information systems, buildings, and related supporting IS infrastructure against threats associated with their physical environment.

The purpose of this policy is to:

- Increase awareness among RSE IS staff of their responsibilities in relation to IS physical and environmental security;
- Ensure that good security principles are reinforced within RSE IS;
- Manage the way in which RSE complies with ISO 270001 Standards.

This policy applies to all personnel of Red Star Express Plc. (employees, contractors, Client and Customers)

SCOPE

The scope of this policy will follow the ISO Standard Information technology — Security techniques — Code of Practice for Information Security Management which has 2 major categories under Physical and Environmental Security:

- ***Secure Areas Objective:***
  The objective of the secure area is to prevent unauthorized physical access, damage, and interference to the organization's premises and information. The physical facility is usually the building, other structure, or environment housing the system and network components.
- ***Equipment Security Objective:***
  The objective of the equipment Security described is to prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

  It also involves those services (both technical and human) that support the operation of the system. The system's operation usually depends on supporting facilities such as

electric power, heating and air conditioning, and telecommunications. The failure or unsatisfactory performance of these facilities may interrupt operation of the system and may cause physical damage to system hardware or stored data.

POLICY

- Appropriate physical and environmental security controls will be implemented at all RSE Information Communication Technology (IS) facilities to protect people, property and other information system resources.
- RSE will adopt a risk management approach when identifying physical and environment controls for IS systems facilities.

POLICY DETAILS

Five major areas of physical and environmental security controls are:

- ✓ Physical access controls
- ✓ Fire safety
- ✓ Supporting utilities
- ✓ Interception of data
- ✓ Mobile and portable systems

Physical Access Controls

Physical access controls restrIS the entry and exit of personnel, equipment and media from an area, such as an office building, suite, data centre, or room containing a LAN server. The objectives of physical access controls may be in conflIS with those of life safety. Life safety focuses on providing easy exit from a facility, particularly in an emergency, while physical security strives to control entry. In general, life safety must be given first consideration, but it is usually possible to achieve an effective balance between the two goals. Physical access controls, include badges, memory cards, guards, keys, true-floor-to-true ceiling wall construction, fences, and locks. Details of this has been described in the Data Centre/Server room Access Control

Fire Safety Factors

Building fires are an important security threat because of the potential for complete destruction of hardware and data, the risk to human life, and the pervasiveness of the damage. Fire extinguisher has been put in place to help first safe attempt

Failure of Supporting Utilities

Information systems and the people who operate them need to have a reasonably well-controlled operating environment. Consequently, failures of heating and air conditioning systems will usually cause a service interruption and may damage hardware and possibly even a loss of information. These utilities are composed of many elements, each of which must function properly. Periodic service checks of the cooling system have been put in place to ensure this.

Interception of Data

Depending on the type of data a system processes, there may be a significant risk if the data is intercepted. There are three routes of data interception: They are: **Direct observation**, **interception of data transmission**, and **electromagnetic interception**.

- Direct Observation: System terminal and workstation display screens may be observed by unauthorized persons**.** To prevent this, ensure you lock your systems when you need to move away temporarily also ensure no one is watching over your shoulder when working on very sensitive documents. Be security Conscious.

- Interception of Data Transmissions: If an interceptor can gain access to data transmission lines, it may be feasible to tap into the lines and read the data being transmitted. Interceptors could also transmit spurious data on tapped lines, either for purposes of disruption or for fraud. To minimize this risk, we need to ensure data transmission lines are properly secured, either laid underground, kept in secured locations or set to be watch over by guards where possible and/or where interception risk is high.

• Electromagnetic Interception: Systems routinely radiate electromagnetic energy that can be detected with special-purpose radio receivers. The trend toward wireless (i.e., deliberate radiation) LAN/WAN connections may increase the likelihood of successful interception. To prevent this, we must **ensure strong authentication mechanism (Password) is put in place**

Mobile and Portable Systems

The analysis and management of risk usually has to be modified if a system is portable, such as a laptop computer. Encryption of data files on mobile and portable equipment may be a cost-effective precaution against disclosure of confidential information if a laptop computer is lost or stolen. Portable and mobile devices share an increased risk of theft and physical damage as well as the risk of being "misplaced" or left unattended. Secure storage of laptop computers is often required when they are not in use. To minimize this risk, Desktops are used majorly for major information and data processing and security.

APPLICATION / SOFTWARE (OS) MANAGEMENT

Policy

Server's operating systems will be secured to authorize personnel only. Corporate operating systems and databases will be standard across the systems/servers.

Security of access to the operating system on the servers is the direct responsibility of the System Mgr. and databases on the servers are the direct responsibility of the System Mgr. and application Manager. Access to the database management system will be limited to the application Mgr.

Creation of new accounts to access the operating systems and application will be based on the user account request form/email approved by Unit head/HR Manager/Head of Department

SUN Accounting

Access to the database management system for SUN Accounting will be limited to the Application Mgr. / System Mgr.

Creation of new accounts to access the SUN Accounting application is the direct responsibility of the IS Mgr. and whoever the IS Mgr. Assigns the responsibility.

Human Manager

Access to the database management system for **Human Manager w**ill be limited to the IS Mgr.

Creation of new accounts to access the **Human Manager application** is the direct responsibility of the IS Mgr.

SmartStarnet & StarnetPro

Access to the database management system for **StarnetPro** will be limited to the System Mgr. and Information and Communication Technology (IS) Manager.

Creation of new accounts to access the **StarnetPro** application is the direct responsibility of the **IS** Mgr. / Web Application developer

Service Quality Index

Access to the database management system for **Service Quality Index w**ill be limited to the System Mgr. and Information & Telecommunication Manager (IS MGR.)

Creation of new accounts to access the **Service Quality application** is the direct responsibility of the **IS** Mgr.

Smart DSS Green/Pink DSS Reconciliation

Access to the database management system for **Green/Pink DSS Reconciliation** will be limited to the System Mgr. And Information & Telecommunication Manager (IS MGR.)

Creation of new accounts to access the **Green/Pink DSS Reconciliation** application is the direct responsibility of the IS Mgr.

Service Rating

Access to the database management system for **Service Rating w**ill be limited to the System Mgr. and IS Mgr.

Creation of new accounts to access the **Service application** is the direct responsibility of the **IS** Mgr.

Creation of User account to access any other company application will be the responsibility of the IS Mgr. and any other person so assigned. This creation should be backed up with an approved request through email or hard copy. The approval can either be from the unit head or HR

INFORMATION SECURITY ORGANIZATION - ANTIVIRUS

PURPOSE

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Red Star Express in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of Red Star Express is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by Red Star Express employees to help achieve effective virus detection and prevention.

SCOPE

This policy applies to all computers that are connected to the Red Star Express network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally-owned computers attached to the Red Star Express network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

GENERAL POLICY

1. Currently, Red Star Express has MCAFEE Endpoint Protection Enterprise License. Licensed copies of MCAFEE Endpoint Protection can be obtained at a shared folder on the antivirus server. The most current available version of the anti-virus software package will be taken as the default standard.

2. All computers attached to the Red Star Express network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

3. Any activities with the intention to create and/or distribute malicious programs onto the Red Star Express network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strISly prohibited.

4. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the IT department immediately at it@redstarplc.com. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

5. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IS Unit.

6. Any virus-infected computer will be removed from the network until it is verified as virus-free.

RULES FOR VIRUS PREVENTION

1. Always run the standard anti-virus software provided by Red Star Express.

2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

3. Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.

4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

5. Files with the following filename extensions are blocked by the e-mail system: .exe, .com, .bat. Business-critical files with special extension can be zipped and sent as email attachment

6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

7. Avoid direct disk sharing with read/write access. Always scan a floppy diskette for viruses before using it.

8. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

9. Back up critical data and systems configurations on a regular basis and store backups in a safe place.

10. Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

IT DEPARTMENT RESPONSIBILITIES

The following activities are the responsibility of the Red Star Express IS Unit:

1. The IT department is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be posted at Intranet Site. Check one of these locations regularly for updated information.

2. The IT department will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use. Automatic updates from antivirus server are available for computers at the HQ, while computers in remote locations connect directly to internet for updates.

3. The IT department will apply any updates to the services it provides that are required to defend against threats from viruses.

4. The IT department will install anti-virus software on all Red Star Express owned and installed desktop workstations, laptops, and servers.

5. The IT department will assist employees in installing anti-virus software according to standards on personally-owned computers that will be used for business purposes. The IT department will provide anti-virus software in these cases.

6. The IT department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

7. The IT department will perform regular anti-virus sweeps of Antivirus Server outdated files.

8. The IT department will attempt to notify users of Red Star Express systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

DEPARTMENT AND INDIVIDUAL RESPONSIBILITIES

The following activities are the responsibility of Red Star Express departments and employees:

1. Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.

2. Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

3. All employees are responsible for taking reasonable measures to protect against virus infection.

4. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the Red Star Express network without the express consent of the IT department.

ENFORCEMENT

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

INFORMATION SECURITY INCIDENT MANAGEMENT POLICY.

DEFINITIONS

Information Security Incident

An Information Security Incident is the occurrence or development of an unwanted or unexpected situation which indicates either:

a) A possible breach of an information security framework policy **or**

b) A failure of information security controls which have a significant probability of compromising business operations.

Examples of Information Security Incidents include (but are not limited to):

- Direct loss or theft of Classified Information (e.g. papers taken from car, post intercepted, un-authorized download)
- Loss or theft of equipment used to store Classified Information (e.g. laptop, smartphone, USB stick)
- Accidental or un-authorized disclosure of 'Confidential' or 'Highly Confidential' Classified Information (e.g. via misaddressed correspondence or incorrect system permissions/filter failure)
- Corruption or un-authorized modification of vital records (e.g. alteration of master records)
- Computer system or equipment compromise (e.g. virus, malware, denial of service attack)
- Compromised IT user account (e.g. spoofing, hacking, shared password)
- Break in at a location holding Classified Information or containing critical information processing equipment such as servers

PURPOSE

The purpose of this policy is to ensure a consistent and effective approach to the management of Information Security Incidents, including communication on security events and weaknesses. It enables the efficient and effective management of Information Security Incidents by providing a definition of an Information Security Incident and establishing a structure for the reporting and management of such incident.

SCOPE

This policy applies to all members of Staff with reference to all information held by or on behalf of the Organization.

RELATIONSHIP WITH EXISTING POLICIES

This policy forms part of the Information Security Management Framework. It should also be read in conjunction with the Managing and Reporting Concerns.

POLICY STATEMENT

Information Security Incidents shall be reported promptly and responded to in a quick, effective and orderly manner in order to reduce the negative effect of incidents, to repair damage and to inform policy and mitigate future risks.

POLICY

- All members of the Staff shall be made aware of the procedure for reporting Information Security Incidents and their responsibility to report such incidents.
- All Information Security Incidents shall be reported promptly to the Service Desk in accordance with the Information Security Incident Reporting Procedure.
- All Information Security Incidents shall be managed in accordance with the Information Security Incident Management Response Procedure. The severity of the incident shall be assessed and the management response shall be proportionate to the threat.
- Key information about serious Information Security incidents, including the impact of the incident (financial or otherwise), shall be formally recorded and the records shall be analyzed in order to assess the effectiveness of information security controls.
- New risks identified as a result of an incident and shall be assigned to the relevant risk owner and unacceptable risks shall be mitigated promptly in accordance with the Organization's risk management processes.
- Relevant staff shall be trained in digital evidence collection, retention, and presentation, in accordance with legislative or regulatory obligations.
- Serious incidents shall be reported to the appropriate external authorities where relevant by authorized individuals.

RESPONSIBILITIES

- All members of Staff are responsible for reporting actual or suspected Information Security Incidents to the relevant internal contact as soon as possible in accordance with the Information Security Incident Reporting Procedure
- Contractors using the Organization's information systems and services shall be required to note and report any significant information security weaknesses in those systems or services.

- The responsibility for responding to Information Security Incidents shall be as set out in the Information Security Incident Management Procedure.
- The responsibility for reporting serious Information Security Incidents to external authorities lies with the Senior Information Risk Owner unless otherwise delegated in the Information Security Incident Management Procedure.

COMPLIANCE

- Failure to report an Information Security Incident and any other breach of this policy shall be considered to be a disciplinary matter and shall be reported to the Senior Information Risk Owner to be addressed under the relevant disciplinary code.
- Compliance with this policy should form part of any contract with a third party that may involve access to Company's networks, computer systems or data. Failure by contractors to comply with clause 7.2 of this policy may constitute an actionable breach of contract.

A *serious Information Security Incident* is an incident whose impact, if unmanaged, has the potential to reach Moderate or above on the Organization's Risk Measurement Criteria.

Classified Information is information that is confidential, highly confidential or requires enhanced protection to ensure integrity or availability due to its nature.

SERVER ROOM/DATA CENTRE POLICY AND PROCEDURE

INTRODUCTION

The procedures described in this document have been developed to maintain a secure Server Room OR Data Centre environment and must be followed by all working in the Server room and IS staff. It is also important that all within the organization understand and agree with this policy and procedure. The server room or data centre of any organization is the backbone of that organization. Its security must be ensured.

OVERVIEW

Security of the server room and all equipment in the server room is the Responsibility of the IS department. The following are the general requirements, policies and practices that govern access to this sensitive area, for which the IS department has responsibility. It is important that all IS staff and possible business associates follow these policies and practices. Failure to do so could attract some penalty to assigned officer in charge.

PRIMARY GUIDELINES

The "Server room" is a restrISed area to all non IS Staff. It requires a much greater level of control than any other rooms or office. Only those individual who are expressly authorized to do so may enter this area. Access privileges will be granted to individuals who have a legitimate business need to be in the server room.

POLICY

LEVELS OF ACCESS TO THE DATA CENTRE

There are 3 "Levels of Access" to the Server Room

ADMIN ACCESS–

The Admin access is granted to one person in the IT department usually the IS manager or any other person assigned by him/her. The administrator has the right to grant access to others as agreed within the contents of the departmental data centre/server room Policy and procedure. The Administrator can also remove access or delete user access as deemed fit. She/he shall be held responsible for whatever goes wrong in the data centre. The Administrator will have the record of all staff with access and shall ensure compliance.

GENERAL ACCESS

This access is given to people who have free access authority into the Server room. General Access is granted to the IS staff whose job responsibilities require that they have access to the area. Individuals with General access to the area may allow properly authorized individuals escorted access to the data centre. If a person with General Access allows Escorted access to an

individual the person granting access is responsible for escorting the individual granted access and seeing to it the protocol is followed.

ESCORTED ACCESS

Sometimes, non IT and unauthorized person such as vendors, Clients may require access to the server room. The escorted access given to people who have a legitimate business need for infrequent access to the server room or data centre is closely monitored. Vendors or client activities that have no direct business with the server room and/or equipment should be attended to outside the server room. Individuals with Escorted Access will not be issued a door combination to access the data centre with. A person given Escorted Access to the area must sign in and out under the direct supervision of a person with General Access, must provide positive identification upon demand, and must leave the area when requested to do so.

SERVER ROOM DOOR

All doors to the server room must remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary in order to:

- Allow officially approved and logged entrance and exit of authorized individuals

- Permit the transfer of supplies/equipment as directly supervised by a person with General Access to the area

- Prop open a door to the server room ONLY if it is necessary to increase airflow into the server room in the case on an air conditioning failure. In this case, staff personnel with General Access or Admin access must be present and limit access to the Data Centre.

IS ASSET MANANGEMENT POLICY

An asset is anything that is of value to the organization. Asset management, broadly defined, refers to any system that monitors and maintains things of value to an entity or group. It may apply to both tangible assets such as buildings and to intangible concepts such as intellectual property and goodwill.

The IS asset management policy deals with analysing and attaining the necessary level of protection of IS assets within Red Star Express Plc. It is a systematic process of operating, maintaining, upgrading, and disposing of IS assets cost-effectively.

OBJECTIVES

The typical objectives of the IS asset management policy are

- To identify and create an inventory of all IS assets
- Establish an ownership on all assets identified
- Establish a set of rules for the acceptable use of assets
- Establish a framework for classification of assets
- Establish an asset labeling and handling guideline.

SCOPE

The IS asset management policy shall cover all IS asset type as classified below within the Company

ASSET TYPE	
Hardware IS Assets	Computers, Printers, Servers, UPS, Inverters etc.
Software IS Asset	Software codes, Applications, Operating Systems, Development tools etc.
STAFF (IS Employees)	Skills and Experience

POLICY FOCUS

- All IS assets shall be clearly identified, documented and regularly updated quarterly in an asset register
- All IS assets shall have designated owners and custodians (department, Subsidiary) listed in the asset register
- All assets will have the respective CIA (Confidentiality, Integrity and Availability) rating established in the asset register
- All custodian or users shall use IS assets according to the acceptable use of assets procedures
- All IS assets shall be classified according the asset classification guideline of the Unit

IS ASSET CLASSIFICATION METHOD

The asset is classified in order to provide an appropriate level of protection for a certain category of assets. It is classified in terms of its value, requirements, Time of Purchase, expected year of End-of-Life, depreciating Value and criticality to the business operations of Red Star Express Plc. Etc.

ASSET LABELING

All IS assets shall be labelled physically / electronically according to the information labelling and handling procedures of Red Star Express Plc. currently being handled by the Audit Unit/department. The asset owners (IS unit, Subsidiaries and Departments) shall ensure that their assets are appropriately labelled for ease of identification.

ASSET DEPRECIATION AND DISPOSAL

Depreciation is based on the capitalised cost and is calculated using the straight-line depreciation method. Assets are depreciated from the date the asset is brought into use. Depreciation value for most IS equipment, ranging from computers, UPS, Printers, Servers, Mobile Scanners, is put at an average of 25% per year hence implies that item life cycle will be 4 years. IS has also adopted a disposal of asset policy as outlined below.

DISPOSAL OF ASSETS

IS Assets may be available for disposal for a number of reasons, e.g.

- Beyond repair
- No longer required due to changed procedures or functions
- Not capable of running required software
- No longer complying with Health and Safety requirements

All requests for disposal must be submitted to the IS Manager for due approval who will forward to the Management account team and then approved by the relevant committee in accordance with the Red Star Express Asset disposal policy and the best possible value must be obtained in the disposal of assets.

Acceptable methods of disposal are

- Private Sale

  To ensure a fair price is received, a market evaluation should be obtained. The sale should be publicized appropriately, via advertising or e-mailing and could be sold to the first person to make an offer or via sealed bids, as appropriate.

- Donation to an appropriate organization

  All donations must be approved by the appropriate authorities

- Recycled or Destroyed

  IS Items with no market value or no use to another organization should be appropriately and safely destroyed. The asset disposal should be approved by appropriate authorities

General disposal procedures

- Identify asset for disposal
- Determine market value
- Management approve disposal
- Select the best disposal method
- Record disposal in the asset register

Sale or donation of IS equipment - specifics

- All hard disc contents should be erased and re-installed
- The recipient of the equipment should be advised in writing that Red Star Express Plc. will not be liable for and Health and Safety issues surrounding the use of the equipment

CHANGE MANAGEMENT PROCEDURE

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

In order to fulfil this policy, the following statements shall be adhered to:

Operational Procedures

The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

At a minimum the change control process should include the following phases:

- Logged Change Requests;
- Identification, prioritization and initiation of change;
- Proper authorization of change;
- Requirements analysis;
- Inter-dependency and compliance analysis;
- Impact Assessment;
- Change approach;
- Change testing;
- User acceptance testing and approval;
- Implementation and release planning;
- Documentation;

Documented Change

All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.

Change Classification

All change requests shall be prioritised in terms of benefits, urgency, effort required and potential Impact on operations.

Testing

Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

Changes affecting SLA‘s

The impact of change on existing SLA’s shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

Version control

Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.

Approval

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

Communicating changes

All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

Implementation

Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

Fall back

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

Documentation

Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.

ACCESS CONTROL

The general access control to all IS facility has been described in the physical and Environmental control policy of this handbook. This however shall deal with implementation of access controls across all electronic forms of information processing systems like operating systems, applications, networks/internet, mobile platforms, Computers, Servers etc.

The objective of the asset access control policy is to establish a procedure for user registration and de-registration, establish a procedure to grant the correct level of access privilege, establish a procedure to control password use, password change and password removal, establish a procedure for managements review of access rights, establish a procedure for unattended equipment, maintain a clear desk policy.

User Registration Policy

Without proper policies to govern user registration, unauthorized people can gain access to confidential company information and leak it out causing harm to the organization economic status and repute. IS has established a user registration procedure which shall include controls for all Hardware, operating systems and applications access as follows

- All users shall have a unique user ID based on a standard naming convention
- A formal authorization process shall be defined and followed for provisioning of user IDs.
- An audit trail shall be kept of all requests to add, modify or delete user accounts/IDs
- User accounts shall be reviewed at regular intervals

- Employee shall sign a privilege form acknowledging their access rights
- Access rights will be revoked for employee changes or leaving jobs
- Privileges shall be allocated to individuals on a 'need-to-have' basis.
- A record of all privilege accounts shall be maintained and updated on regular basis
    - **Access to Servers:** IS unit is the custodian of all Servers in Red Star Express. Not all support staff has access to the various servers. The IS manager shall of his own discretion assign right to support staff and only authorized staff within the unit shall access the respective Servers (DC and AD Servers, Various Applications, FTP etc.)

    - **Access to Computers:** All registered users shall have access to a Computer and shall be assigned same at the manager's discretion or where the job description clearly defines a need-to-have. Users are created and registered by IS on HR's authorization

    - **Access to Application:** All applications have various level of authorization and shall be granted based on request and approval. The IS Manager shall maintain the overall Administrator right and can of his discretion assign same right to anyone within the unit

    - **Internet Access:** Right to use of the internet facility shall be based on request and approval from respective managers with justification that user requires access to carry on job function. This is controlled and checked by Sophos equipment.

RESPONSIBILITY AND COMPLIANCE

The IS unit shall be responsible for the Policy and Ensure mandatory compliance to the set out policy. All Staff of Red Star Express Plc. with the minute access to IS service of any type and in possession of any IS asset must comply. If there shall be any waiver and/or exception to the set policy, it shall be at the discretion of the IS Manager Only

HUMAN RESOURCE SECURITY POLICY

OBJECTIVE

Human resources policies and practices should reduce the risk of theft, fraud or misuse of information and Communication facilities by employees, contractors and third-party users.

SCOPE

Red Star Express IS human resources security policies, taken as a whole, extends to all the persons within and external to the IS unit that do (or may) use information or information processing facilities. This include: Computers, UPS, Printers and Emails, Applications (SUN, Vision, CUSSIT, and StarnetPro etc.). The Unit shall

- Ensure awareness of information security threats and concerns, and the necessary steps to mitigate those threats; by sending email notifications.
- equip all persons to support organizational **privacy and security policies** in the course of their normal work, through appropriate training and awareness programs that reduce human error; E.g. Includes turning off Electrical switch at the close of work, Backing up personal flies to external drives as a safety measure
- Ensure IS Staff exit the organization, or change employment responsibilities within the organization, in an orderly manner.
- Ensue Staff fully understand the security responsibilities and liabilities of their role(s);

Roles and responsibilities •
The Security roles and responsibilities of employees, contractors and third-party users of IS facility is defined and documented as follows;

- To protect all information assets from unauthorized access, use, modification, disclosure, destruction or interference; as defined in the access control policy, password policy, user registration and authorization.
- To report security events, potential events, or other risks to the organization and its IS assets; and advise on necessary precaution

Pre-employment screening for IS Staff • Appropriate background verification checks ("screening") for all candidates for employment, contractor status, or third party user status, shall be carried out by the IS through the organization or appropriate third parties. This will include:

- Ensuring Prospective IS staff, Contractors, vendors, commensurate with the organization's business needs, and with relevant legal-regulatory-certificatory requirements.
- Putting into account the classification(s)/sensitivity (ies) of the information or information processing facilities to be accessed, and the perceived risks;
- Taking into account all privacy, protection of personal data and other relevant employment legislation; and
- Includes, where appropriate, components such as identity verification, character references, CV verification, criminal and credit checks.

Terms and conditions of employment • Employees, contractors, and third party users shall agree to and sign a statement of rights and responsibilities for their affiliation with Red Star Express Plc. IS unit, including rights and responsibilities with respect to information privacy and security. The following shall be properly checked and defined before final employment of any IS staff.

- The scope of access and other privileges the person will have, with respect to the organization's information and information processing facilities; Depending on the level of the employed staff, Scope of access shall be at the discretion of the IS manager
- The person's responsibilities, under legal-regulatory-certificatory requirements and organizational policies, specified in that or other signed agreements. This shall be given by the company's HR Manager or Executive
- Procedures for handling sensitive information, both internal to the organization and that received from or transferred to outside parties; This shall depend on the information or asset involved and guideline shall be given in black and white and signed accordingly.
- Red Star Express code of conduct or code of ethics to the employee, contractor or third party; IS Employees have the sole responsibility to support users (internal and external customer) on the use of IS service and infrastructure, The Code of conduct is to ensure continuous customer satisfaction and adhere to the IS support Policy section outlined in

this Handbook; Vendors shall supply IS equipment based on requirement and approved standard as signed for. Code of conduct of Vendors and contractors requesting access to the IS facility shall be in line with the Access Policy outlined in the Handbook.

- Where it is necessary for an IS employee, vendor, contractor to use or access IS asset outside the organization; A writing and signed Terms and condition of use and access must be in place and disciplinary measures according to the Managers discretion shall be taken against violations

IS Management responsibilities •

The core responsibility is to require employees, contractors and third party users to apply security controls in accordance with established policies and procedures of the Unit and organization as a whole. Management shall do the following

- Inform all employees, contractors and third party users of their information security roles and responsibilities, prior to granting access to sensitive information or information systems
- Provide all employees, contractors and third parties with guidelines/rules that state the security expectations of their roles within the organization;
- Achieve an appropriate level of skills and qualifications, sufficient to execute outlined security controls;
- Assure conformity to the terms and conditions of employment related to privacy and security;
- Motivate adherence to the privacy and security policies of the organization, such as with an appropriate sanctions policy; and
- Mitigate the risks of a failure to adhere to policies, by ensuring that all persons have appropriately-limited access to the organization's information and information facilities (see **Access and Password Policy control in this Handbook**).

Information Security Awareness, Education and Training:

All IS employees and, where relevant, contractors and third party users, should receive appropriate awareness training in and regular updates of organizational policies and procedures relevant to their job functions. This will include:

- A formal induction process that includes information privacy and security training, prior to being granted access to IS information or information systems; and
- Ongoing training in security control requirements, legal-regulatory-certificatory responsibilities, and generally accepted security procedures, suitable to the person's rules and responsibilities.

Disciplinary process •

Depending on the offence, disciplinary process for employees who have committed a security breach shall be in accordance to Red Star Express Plc. Procedure and in the event such breach is not provided for, Discipline shall be at the discretion of the management team. This shall be applied after;

- Appropriate investigations have been carried out to establish the offence
- Queries and response has been gathered
- Careful consideration of factors such as the nature and gravity of the breach, its impact on operations, whether it is a first or repeat offense, whether or not the violator was appropriately trained, whether or not the violator exercised due care or exhibited negligence.

Termination responsibilities • Responsibilities and practices for performing employment termination of IS employee shall be in line with Red Star Express Condition for employee Termination Policy. Termination processes that ensure removal of access to all information resources shall be on violation of rights. E.g. Access to internet facility shall be revoked for users found to visit prohibited sites.

Return of assets: All IS employees, contractors and third parties should return all of the organization's information and physical assets in their possession upon termination of the employment relationship or contract. There shall be;

- A formal process for return which shall be a checklist against inventory of the organization's hardware, software and data media;
- Where the employee, contractor or third party uses personal equipment, requirements for secure erasure of software and data belonging to the organization.

Removal of access rights

All access rights to information and information processing facilities shall be removed upon termination of the employment or contractual relationship.

COMMUNICATIONS AND OPERATIONS MANAGEMENT POLICY-
NETWORK ACCESS, EMAIL, INTRANET AND INTERNET SECURITY POLICY

POLICY STATEMENT

RED STAR PLC will ensure the protection of the IT service (*including any information systems and information processing equipment used by the company*) against malware and malicious and mobile code.

Only authorized changes will be made to the IT service (*including any information systems and information processing equipment*). Information leakage will be prevented by secure controls.

PURPOSE

This policy covers the key areas in day to day operations management of the RED STAR PLC IS services.

This policy subsists to protect the information and IT Infrastructure owned by RED STAR PLC and to ensure people are aware of any restrISions in their use.

Change Management

Changes to the Company's operational systems must be controlled with a formally documented change control procedure. The change control procedure should include references to:

- A description of the change and business reasons.
- Information concerning the testing phases.
- Impact assessment including security, operations and risk.
- Formal approval process.
- Communication to all relevant people of the changes.
- Procedures for aborting and rolling back if problems occur.
- Process for tracking and audit.

Capacity Planning

All RED STAR PLC IT infrastructure components or facilities are covered by capacity planning and replacement strategies to ensure that increased power and data storage requirements can be addressed and fulfilled in a timely manner.

Key IT infrastructure components include, but are not restrISed to, the following:

- File servers.
- Domain servers.
- E-mail servers.
- Web servers.
- Printers.
- Networks.
- Environmental controls including air conditioning.

PROTECTION AGAINST MALICIOUS AND MOBILE CODE

Appropriate steps are taken to protect all RED STAR PLC IT systems, infrastructure and information against malicious code. Effective and up-to-date anti-virus software is run on all servers and PCs. RED STAR PLC staff is responsible for ensuring that they do not introduce

malicious code into RED STAR PLC IT systems – as stated within the Software Policy. Where a virus is detected on a RED STAR PLC system, the individual must contact the IS Helpdesk.

INFORMATION BACKUP

Regular backups of essential business information must be taken to ensure that the RED STAR PLC can recover from a disaster, media failure or error. An appropriate backup cycle must be used and fully documented. Any 3rd party that stores RED STAR PLC information must also be required to ensure that the information is backed up. Full back up documentation, including a complete record of what has been backed up along with the recovery procedure, must be stored at an offsite location in addition to the copy at the main site and be readily accessible. This must also be accompanied by an appropriate set of media tapes and stored in a secure area. The remote location must be sufficiently remote to avoid being affected by any disaster that takes place at the main site.

WIRELESS NETWORKS

Wireless networks must apply controls to protect data passing over the network and prevent unauthorized access. Encryption must be used on the network to prevent information being intercepted. WPA2 should be applied as a minimum.

A. NETWORK ACCESS

INTRODUCTION

The [RED STAR EXPRESS PLC] network infrastructure is provided as a central utility for all users of [RED STAR EXPRESS PLC] Information Resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet [RED STAR EXPRESS PLC] demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

PURPOSE

The purpose of the [RED STAR EXPRESS PLC] Network Access Policy is to establish the rules

for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of [RED STAR EXPRESS PLC] information.

AUDIENCE

The [RED STAR EXPRESS PLC] Network Access Policy applies equally to all individuals with access to any [RED STAR EXPRESS PLC] Information Resource.

DEFINITIONS

Information Resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), I phones, distributed processing systems, network attached, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information & Telecommunication Manager (IS MGR.): Responsible to the State of Red Star Express Plc. for management of the RED STAR EXPRESS's information resources. The designation of an RED STAR EXPRESS information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of RED STAR EXPRESS PLC's information activities, and ensure greater visibility of such activities. The ISM has been given the authority and the accountability by the Management to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the RED STAR EXPRESS PLC

System Network Manager: Responsible to executive management for administering the information security functions within the RED STAR EXPRESS is the internal and external point of contact for all information security matters.

Information Technology (IT): The name of the RED STAR EXPRESS PLC Unit responsible for computers, networking and data management.

NETWORK ACCESS POLICY

- Users are permitted to use only those network addresses issued to them by [RED STAR EXPRESS PLC] **System Network Manager**.
- All remote access (dial in services) to [RED STAR EXPRESS PLC] will be either through an approved modem pool or via an Internet Service Provider (ISP).
- Remote users may connect to [RED STAR EXPRESS PLC] Information Resources only through an ISP and using protocols approved by [RED STAR EXPRESS PLC].
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the [RED STAR EXPRESS PLC] network without [RED STAR EXPRESS PLC] **System Network Manager** Approval.
- Users must not install network hardware or software that provides network services without [RED STAR EXPRESS PLC] **System Network Manager** Approval.
- [RED STAR EXPRESS PLC] computer systems that require network connectivity must conform to [RED STAR EXPRESS PLC] **System Network Manager** Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, [RED STAR EXPRESS PLC] users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the [RED STAR EXPRESS PLC] network infrastructure.
- Users are not permitted to alter network hardware in any way.
- There is no guarantee of privacy in using the Internet/Intranet, including e-mail communication. RED STAR PLC reserves the right to monitor all user Internet/Intranet communications and examine all information collected, created and/or generated as a result of using RED STAR PLC Internet/Intranet including any files, messages, printouts, removable media, or other material in order to monitor users' compliance with this policy.

DISCIPLINARY ACTIONS

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or casuals; Additionally, individuals are subject to loss of [RED STAR EXPRESS PLC]

Information Resources access privileges, civil, and criminal prosecution.

Additionally, individuals are subject to loss of [RED STAR EXPRESS PLC] Information Resources access privileges, civil, and criminal prosecution.

B. EMAIL, INTRANET AND INTERNET SECURITYPOLICY

INTRODUCTION

All employees are expected to sign and abide by this policy. Signed agreement forms are to be provided to facility's IS Unit. After completion, the form will be filed in the individual's human resources file (for permanent employees), or in a folder specifically dedicated to Internet access (for contract workers, etc.), and maintained by the IT department.

The ***Intranet and Internet Security Policy*** applies to all Intranet/Internet users (including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners and vendors) who access the Internet through Red Star Express computing or networking resources. Intranet/Internet users are expected to be familiar with and to comply with this policy. Users are also expected to use their common sense and exercise good judgment while using Internet services.

Violations of the *Intranet and Internet Security Policy*, including but not limited to violation of information specified herein will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination. Additionally, Red Star Express may at its discretion seek legal remedies for damages incurred as a result of any violation. Red Star Express may also be required by law to report certain illegal activities to the proper enforcement agencies.

GENERAL SECURITY POLICY

Users are to:

- Use computer systems for solely corporate business purposes.

- Maintain the privacy and confidentiality of all confidential and institutional data. (See Information Classification Section)
- Use unique user-IDs and personal non-trivial secret passwords to access computer systems. Users are responsible for all activities occurring with their User-IDs.
- Log out of all systems when leaving a computer system unattended.
- Report information security violations immediately.
- Adhere to virus control procedures. All software to be installed or downloaded from external sources through the Intranet or Internet must be screened with virus detection software before being invoked.
- Refrain from connecting networked workstation to modems without approval. At no time should networked workstations be connected both to the Internet via a modem and to the company network.
- Comply with all third-party software licenses. Any unlicensed software must be immediately removed from company computers.

INFORMATION CLASSIFICATION

Information assets must be identified, classified, and labelled based on the sensitivity to the organization (i.e., the business impact if destroyed, damaged or disclosed). Owners are responsible for classifying information assets. Everyone is responsible to ensure that the appropriate level of protection is consistently applied. Information assets must be classified according to the following scheme:

- Level 1 -- Confidential Information: This class represents important and/or highly sensitive material that is appropriate for only specific employees. Unauthorized disclosure, modification, or destruction of this information could cause serious damage to the company and our clients.
- Level 2 -- Institutional Information: This class represents information important to the company. Its destruction and/or modification could result in serious losses. This information must have controls to ensure its integrity and accuracy. Its use is therefore subject to certain restrISions.

- Level 3 -- UnrestrISed Information: This class represents information that does not fall into one of the above classifications and is appropriate for all company personnel in addition to the general public. This information is not considered confidential, and its disclosure, modification and/or destruction does not need to be controlled.

Information classified as Level 1, log-in passwords and other parameters that can be used to gain access to the company are a few examples of data types which must be encrypted by the approved encryption standard before transmission over the Intranet or Internet. In addition, Level 2 data must be sent encrypted over the Internet. It may be in the clear on the Intranet

ELECTRONIC MAIL POLICY

The electronic mail system is to be used for business purposes only. All messages sent by electronic mail are the property of Red Star Express. Red Star Express reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose. Supervisors may review the electronic mail communications of workers they supervise to determine whether they have breached security, violated company policy, or taken other unauthorized actions. Red Star Express may also disclose electronic mail messages to law enforcement officials without prior notice to the employees who may have sent or received such messages.

Employees must not use an electronic mail account assigned to another individual to either send or receive messages. If there is need to read another's mail (while they are away on vacation for instance), message forwarding and other facilities be used must instead.

Unless the information owner/originator agrees in advance, or unless the information is clearly public in nature, employees must not forward electronic mail to any address outside the company network.
Employees must not create their own, or forward electronic mail messages which may be considered illegal, pornographic, or negatively depISs race, sex or creed.

INTERNET ACCESS POLICY

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Acceptable use of the Internet for performing job functions includes:

- Communication between employees and non-employees for business purposes.
- IT technical support downloading software upgrades and patches.
- Review of possible vendor web sites for product information.
- Reference regulatory or technical information.
- Research.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from clients or business partners, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.

Other specific activities that are strISly prohibited include but are not limited to:

- Accessing confidential information that is not within the scope of one's work.
- Misusing, disclosing without proper authorization, or altering company or personnel information.
- Any unauthorized, deliberate action that damages or disrupts computing systems or networks, alters their normal performance, or causes them to malfunction regardless of location or duration.
- Wilful or negligent introduction of computer viruses, Trojan horses or other destructive programs into company systems or networks or into external systems and networks.
- Unauthorized decryption or attempt at decryption of any system or user passwords or any other user's encrypted files.
- Packet sniffing, packet spoofing, or use of any other means to gain unauthorized access to a computing system or network.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.

- Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IS Unit and the user's manager.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law.
- Deliberate pointing or hyper-linking of the company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation with the aims or policies of Red Star Express.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Acquisition, storage, dissemination, creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any ordering (shopping) of items or services on the Internet.
- Playing of any games.
- Forwarding of chain letters.
- Participation in on-line contest forms of gambling or accepting of promotional gifts.
- Live streaming of music and video on cooperate network.
- Installation of unauthorized programs by IS unit.

AGREEMENT TO COMPLY WITH COMMUNICATION AND OPERATIONS POLICIES

Every staff of Red Star Express Plc. and its Subsidiary who has access to information systems of the company is to comply with the stated policies herein on (***Network***, ***intranet and Internet Security Policy)*** and is binding upon signing with the Human resources in agreement to abide by every law, rules and regulations within the company.

The compliance binds that the staff with access to information systems is responsible for any possession of company information resources and must protect these information resource from unauthorized activities including disclosure, modification, deletion, and usage. Staff must abide to the policies and procedures described therein as a condition of continued employment and that violators of these policies and procedures are subject to disciplinary

measures including privilege revocation and/or employment termination. Disciplinary measures will be at the discretion of the IS Manager, HR Manager and Red Star Managing authorities collectively. Staff must understand that access to company information systems is a privilege which may be changed or revoked at the sole discretion of management. must promptly report all violations or suspected violations of information security policies and procedures to the Corporate Help Desk; IS unit or any authority in charge.

INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE POLICY

Overview

Security can be incorporated into information systems acquisition, development and maintenance by implementing effective security practices. A key part of those practices is that software needs to be monitored and patched for **technical vulnerabilities.** Procedures for applying patches should include evaluating the patches to determine their appropriateness and whether or not they can be successfully removed in case of a negative impact.

Objective

This policy is established to specify the security practices during information system acquisition, development and maintenance, in order to ensure sufficient security in all information systems, and prevent errors, loss, unauthorized modification or misuse of information in the Organization's information systems

Scope

This standard covers the development or acquisition of new information systems, or major modification of existing systems of the Organization. Both in-house developed and outsourced developed systems are covered in this standard.

POLICY STATEMENT

- All statements of business requirements for new information systems or enhancements to existing information systems must specify control and system security requirements.
- Systems security requirements must reflect the business value of the information assets involved.

- Business process owners must ensure that adequate application controls are in place in the applications.
- Applications developed within the Organization must be developed in accordance with an accepted systems development and maintenance methodology, and as per the security requirements reflecting business needs.
- Appropriate controls including audit trails and activity logs must be designed into application systems.
- Cryptographic controls must be implemented in accordance with the Organization's standards and procedures for encryption. The usage of cryptographic controls must comply with applicable laws and regulations.
    1. The Organization must have a defined type of encryption algorithm used and length of cryptographic keys, as per the criticality of the business processes.
    2. The length of the cryptographic keys must comply with applicable cyber laws and regulations.
    3. A legal framework must be developed and enforced for the usage of digital signatures and must comply with applicable cyber laws and regulations.
    4. Non repudiation services shall be used to resolve disputes about occurrence or non–occurrence of an event or action.
- The Organization must identify the secret key techniques and public key techniques to be used, as per the requirements.
- All secret, public and private keys must be protected against modification, destruction and unauthorized disclosure.
- The Organization must have formal standards, procedures and methodology for key management.
- All changes to software in the Production environment should only be made by authorized personnel and should be in accordance with the Organization's Change Management Procedures.
- Software source code must be stored in a physically separated place from the production environment.
- All attempts to access operational software must be logged. The Organization must review the logs at pre-determined intervals.

- Where copies of operational data are used for testing purposes, they must be appropriately de-personalized.
- System test data must be subject to the same level of access controls as the production data from which it was derived or extracted.
- Access to system test data must be logged and monitored on a periodic basis.
- Access to source code libraries must be restrISed in accordance with the Organization's Change Management Procedures.
- Modified source code should be deposited into the library as a new version of the source code. Overwriting or modification of existing source code in the library is expressly prohibited.
- Only the designated and authorized source code librarian (or equivalent) should have 'write' access to the source code library.
- Issue and return of code must be in accordance with the Organization's procedures for this purpose.

SOFTWARE ACQUISITION

1. **Acquisition Planning**

- The Organization's strategy, initiating the planning process, and establishing general practices for planning of the software acquisition, requires to be instituted.
- The functionality that the software should address is to be defined, analyzed and frozen.

2. **Contracting**

- Prospective vendors should be identified.
- Contract requirements should be prepared.
- Once the proposals are received, they should be evaluated.

SECURITY IN DEVELOPMENT AND SUPPORT PROCESS

- The Organization's Change Control Procedures must be compliant with or based on an accepted system development and maintenance methodology.
- System documentation must be updated to reflect changes.
- An audit trail and version control must be maintained for all changes made.

Technical Review of Operating System Changes

- Organization Change Control Procedures must address all changes, enhancements, installation of new software patches and version updates.
- Prior to application of the updates in the production ('live') environment, the Organization must test the operation and compatibility of existing applications with the proposed updates.
- All updates, patches, version changes, etc., must be tested and reviewed for security controls prior to implementation.

RestrISions on Changes to Software Packages

- Modifications to software packages should be discouraged.
- All modifications (including configuration changes, changes to reports, etc.) to software packages must be made in accordance with the Organization's Change Control Procedures.
- All software and hardware must be acquired from trusted sources.
- The Organization must require that the vendor guarantees that the software is free of 'Covert channels' and 'Trojan' code when purchasing the software from third parties.

Outsourced Software Development

- A process must be implemented to verify the vendor's compliance with the Organization's requirements.
- All outsourced developments must adhere to the "Compliance Measurement" Policy of the Organization.
- If third party software is being considered for critical business activity, the Organization must procure the source code from the third party.
- Where the source code is not procured, the third party must provide the source code to an outside party who will hold the source code in escrow each time the source code is revised.

- All documentation must be reviewed by the Organization prior to being released to third parties.

Development of Maintenance Plan

- The maintenance process should be developed by the Organization.
- The Organization requires that all information security projects must be managed in accordance with the Organizations accepted Project Management Methodology.
- The Organization requires that Information Security must be considered as a component of all projects undertaken by or on behalf of the Organization.

IS SERVICE AND SUPPORT POLICY AND PROCEDURE

The IS service and support policy is a guideline to help all employees understand the following

- Essence of IS service and/or support
- Who needs IS service and/or support?
- What should be supported
- Set Standard for System Setup

ESSENCE OF IS SERVICE AND/OR SUPPORT The essence of IS service and support within any organization is to ensure a smooth, continuous service operation, minimize downtime by applying fixes temporal and permanent to any disruption of service arising from the use of IS infrastructure.

It is of high importance to have a stand by support team to ensure business and operation continuity.

WHAT SHOULD BE SUPPORTED?

Red Star Express Plc. has a product brand policy for each IS infrastructure within the company. The IS and Brand is hereby listed below;

IS INFRASTRUCTURE	PRODUCT BRAND	OS

Complete Desktop Computer (Monitor & CPU)	HP ONLY	Windows ONLY
Servers	HP ONLY	Windows Server OS
Printers and Desktop Scanners	HP Only for Mini 3-in-1 Printers, Kyocera for Central or Network Printers, Epson for Billing and Operations.	To be installed on Windows OS and Network printer can be connected to system running other OS where possible
UPS	Blue gate, Mercury, Leums, BPC and APC	N/A
Mobile Scanners	Motorola	Windows OS
Telecommunication Equipment	Various (Ericson, 21Century E1 Line etc.)	ERICSON PB250

WHO NEEDS IS SERVICE AND/OR SUPPORT?

Every user of the above listed product brand within the organization will be supported fully by the IS team

Every other product brand and OS outside the company's brand will be supported by the IS team but not under compulsion and charges may apply where the need be and support staff may not support user except in the event that this policy has been amended to include such brand and necessary supporting applications and infrastructure has been put in place by the company.

Pc/Laptop Setup Checklist Updated June 1, 2016

This checklist will serve as guide in installation of new Pc or Laptop in **Red Star Plc**.

Operating System: Windows 7-10 Professional

☐ **Microsoft windows 7/8**

☐ Set the language setting to keyboard's type you have

☐ Set the systems country location to Nigeria.

☐ Set the time zone to west central Africa.

☐ **Taskbar and start Menu**

☐ Keep the taskbar on top of other windows

☐ Lock the taskbar and show the clock

☐ **Windows updates and patches**

☐ Ensure Pc is setup to take update from internet (Outstations)

☐ **Systems configuration**

☐ Set Computer Name (HQ): UNIT-CPU Serial NUM e.g. TRY-S/N, RSL-S/N, CUS-S/N

☐ Set Computer Name (Outstation): STATION-S/N e.g. ABV-S/N, RSLABV-S/N, PHC S/N

☐ Set Computer Description: RSE-DEPARTMENT e.g. RSE-FINANCE, RSE-OPERATIONS

☐ Set Domain (Head Office): Redstarexpress.local

☐ Set Workgroup (Outstation): RSE-LOCATION. e.g. RSE-ABA, RSE-ABV

☐ Set Workgroup (Personal PC): WORKGROUP

☐ **User's accounts**

☐ Two users accounts should be created: Administrator and Systems users

☐ Administrator should have the administrative right to the systems and has a generic password
(Redstar@1) for Outstation Computers and should be disabled for HQ Computers where the use of Domain account is possible

☐ The system user should have username been the first alphabet of the user's first name and then followed by the surname.

☐ Force the user to change password at next logon

☐ Password BIOS set up for security reasons

☐ Change guest password and disable guest user account

□ **Network**

□ Configure TCP/IP to DHCP

□ Disable firewall for advanced tab

□ **Settings of systems scheduled task**

□ From the control panel: from the event viewer/action menu select properties

For each item (application, security and system) set the log size to 5mb and set overwrite events older than 14 days ON.

□ **Systems Audit**

□ Set the system to perform audit log ON

Account logon events, account management, direct service access, process Privilege use, logon events, object access, policy change

□ **Security centre**

□ Install McAfee anti-virus

□ Disable McAfee firewall

□ Set McAfee update to the internal server

□ **Internet properties**

□ Set the settings for Cyberoam

□ Set the limit of the “Disk space to use for temporary file” to 500MB

□ Set “Days to keep pages in history” to 5 days

□ In the privacy tab, set “block pop-ups” ON

□ In the advance settings click on the “Restore Default “button

□ **Network printer**

□ Install Printer or Set the system to use the nearest network printer

□ **Remote assistance**

□ Install Real VNC control on all computers (except GEC members) and Team Viewer mostly for Outstations

□ **Software**

IS will ensure Setup and Installation of following Software as applicable to the user or Department Ms Office 10, Acrobat Reader, Egrid, COSMOS/EOPs Link, PDF Converter/Printer RSM, FSM, Sure, SUN Link, VISION, Two Additional Browsers Minimum, Starnet2009, SmartDSS, WinRAR

THE DEPARTMENT WILL ADOPT THE FOLLOWING CODE FOR UNIT WITHIN THE HQ

S/N	UNIT	CODE
1	Treasury	TRY
2	Accounting System	ACS
3	Customer Account	CUA
4	Customer Service	CUS
5	Quality and Service Assurance	QSA

REQUIRED	STATUS

6	Mainland Operation	MOP
7	Island (Operations and Debagging)	ISL
8	Audit	ADT
9	Admin	ADM
10	Red Star Logistics (All Department)	RSL
11	Red Star Support (All Department)	RSS
12	Red Star Freight (All Department)	RSF
13	Import	IMP
14	Warehouse	RLW
15	Export	EXP
16	Cooperative	COP
17	Debagging	DBG
18	New Ventures	NVN
19	BULK Mail	BMS
20	Billing	BIL
21	Sales	SAL
22	Human Resources	HRU
23	Legal	LGL
24	Training	TRA
25	Marketing	MKT
26	Key Account	KAC
27	Credit Control Administrator	CCA

Outstation will remain as it is with the Company's adopted abbreviation method. ABV, PHC, ISL, MLD

STICK ON CHECK LIST

OS Win 8 Pro	
System Config Naming Convention	
Admin Disabled or Password Reset	
Join Computer to Domain	
System Audit	
Disable Firewall	
Antivirus	
Printer	
Cyberoam	
MS 10 Office	
Adobe Reader	
Egrid	
COSMOS/EOPs Desktop Shortcut	
PDF Converter	
FSM	
RSM	
SURE	
SUN Link Desktop Shortcut	
VISION	
2 additional Browser	
SmartStarnet2009	
WinRAR	
HR/Human Manager	
Starnet	
SmartDSS	

Name of Engineer: **Signature:**

RISK MANAGEMENT (DATA BACKUP TESTING AND RETENTIONPOLICY

1.0 Overview

This policy defines the backup policy for computers within Red Star Express Plc. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server.

2.0 Purpose

This policy is designed to protect data in Red Star Express Plc. to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

3.0 Scope

This policy applies to all data owned and operated by the Red Star Express Plc.

4.0 Definitions

Backup - The saving of files onto magnetic tape, External Disk drive, Internal Disk drives, Backup Server media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Restore - The process of bringing off line storage data back from the offline media and putting it on an online Server or Test server.

5.0 Timing

Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday, Saturday, and Sunday

Real Time Data replication

6.0 Tape Storage or External Disk

There shall be a set of tapes or external disk for backups of the backups on monthly basis

7.0 Tape Drive Cleaning

Tape drives shall be cleaned monthly before used and the cleaning tape shall be changed monthly.

8.0 Monthly Backups

Every month a backup tape or External disk shall be made using the clean tape or disk from the sets.

9.0 Age of tapes

The date each tape was put into service shall be recorded on the tape. Tapes that have been used must not be reused and replaced with new tapes except for testing.

10.0 Responsibility

The IS Unit manager shall delegate a member of the IS Unit to perform regular backup Log backups monitoring.

The delegated person shall follow a procedure for testing backups and restore data from backups on a quarterly (3 months) basis.

11.0 Testing

The ability to restore data from backups shall be tested at least once per quarter (3 months).

12.0 Data Backed Up

Data to be backed up include the following information:

Data files from **StarNet**Pro Server – Courier Operation

Data files from **SunAccount** Server – For Finance

Data files from **Exchange** Server – Email

System Databases of all the Servers

Systems to be backed up include but are not limited to:

STARNET PRO SERVER – Courier Operation

SUN ACCOUNT SERVER– For Finance

EXCHANGE SERVER – Email

13.0 Restoration

Users that need files restored must submit a request to the help desk/IS Unit approved by Head of department. Include information about the file and year

14.0 Tape Storage Locations

Offline tapes used for monthly backup shall be stored in Montgomery Vaults a fireproof safe.

Data Source Manifest			
Policy Date:	2015	Server Names:	STARNET PRO SUN ACCOUNT EXCHANGE

Type of Backup SOFTWARE Needed

	WINDOWS	MS SQL	Type:	AUTOMATIC TASK SETUP] [BACKUP
	WINDOWS	XLINK PRO REPLICATION	Type:	REPLICATOR
	WINDOWS	SYMANTEC EXE	Type:	REPLICATOR
	WINDOWS	NOVO SOFT HANDY BACKUP	Type:	BACKUP

List of Files/Folders of Backed Up – WEEKLY BACKUP ON EXTERNAL DISK

MONDAY - day 1	
TUESDAY – day 2	
WEDNESDAY- day 3	
THURSDAY- day 4	
FRIDAY- day 5	
SATURDAY- day 6	
[SUNDAY – day 7]	

Offsite

RETENTION	PERMANENTTLY KEEPT ON THE DEVICE	
Offsite Storage:	DISK BACKUP - MONTGOMERY VAULTS BACKUP SERVER AT REMOTE LOCATION	MONTHLY REAL-TIME

COOPORATE COMPLIANCE POLICY AND PROCEDURE

Purpose: To minimize any potential for employees to engage in unlawful conduct affecting the organization, and to assure upon such conduct, that these matters are handled appropriately, including reporting to the appropriate authorities.

Scope: All personnel, whether directly employed or contracted, as well as volunteers and interns.

Policy: It is the policy of Red Star Express to ensure adherence to all pertinent federals, state and local laws, regulations and policies and to provide a mechanism for preventing and reporting any breach of those laws or regulations.

Procedure:

1. Designate a compliance officer as a point of contact that is responsible for ensuring that all compliance related activities are being performed. Will be following up and documenting on audits, complaints, investigations and training.

2. Conduct review of policies and procedures in all high risk areas to enhance compliance.

3. Internal and external monitoring and auditing for high-risk areas.

4. Empower all involved parties to prevent, detect, respond to, report and resolve conduct that does not conform to applicable laws and regulations, and the organization's ethical standards/code of conduct.

5. Determine modes of communication to be implemented for staff members to voice questions, concerns and complaints. Train and educate all staff, volunteers, interns and vendors as to the proper procedure to express the complaint.

6. Respond appropriately to detected offenses and develop plan of corrective action both internally and externally.

7. Document in the Compliance Plan to reflect all complaints made and actions taken.

APPENDIX A

IS UNIT STAFF LIST

1. GBENGA AKANDE
2. KIKELOMO OLAWALE
3. BAMGBELU ABIMBOLA
4. ABDULLAHI IBRAHIM
5. AYANDIPE JOHN
6. BUKOLA ADEKUNLE
7. LAWAL ABIODUN WALE
8. OLUWASEUN ABOLARIN
9. OLAONIPEKUN QUDUS

DECLARATION OF UNDERSTANDING AND AGREEMENT TO ALL POLICY

I, [_____], have read, understand, and agree to adhere to Red Star Express's IS policy and procedure stated in this handbook

Unit_____ Dept. _____

Signature and Date: _____

Unit Head Name/Signature: _____

Dept. Head Name/Signed: _____

Kindly make two copies of declaration and sign off page and submit one each to IS and HR unit