

**SELCOM PAYTECH LTD**

**Disaster Recovery Plan**





**TABLE OF CONTENTS**

- 1. Introduction ..... 1**
  - Definition of a Disaster ..... 1
  - Purpose ..... 1
  - Scope ..... 1
- 2. Disaster Recovery Teams & Responsibilities ..... 2**
  - Disaster Recovery Lead ..... 3
  - Network IT Team ..... 4
  - Applications Team ..... 5
  - Operations Team ..... 6
  - Senior Management Team ..... 7
- 3. Recovery Facilities ..... 8**
  - Description of Recovery Facilities ..... 8
  - Operational Considerations ..... 10
  - Data and Backups ..... 11
- 4. Communicating During a Disaster ..... 12**
  - Communicating with the Authorities ..... 12
  - Communicating with Employees ..... 12
  - Communicating with Vendors ..... 13
- 5. Dealing with a Disaster ..... 14**
  - Disaster Identification and Declaration ..... 14
  - DRP Activation ..... 15
  - Assessment of Current and Prevention of Further Damage ..... 15
  - Standby Facility Activation ..... 16
- 6. Plan Testing & Maintenance ..... 17**
  - Maintenance ..... 17
  - Testing ..... 18
- 7. Document Control ..... 18**



## 1. Introduction

Disaster Recovery Plan (DRP) captures, in a single repository, all of the information that describes Selcom's ability to withstand a disaster as well as the processes that must be followed to achieve disaster recovery. The reason to implement a DR plan to achieve uptime for the clients and vendors connected to Selcom Network Systems.

### Definition of a Disaster

A disaster can be caused by man or nature and results in Selcom's IT department not being able to perform all or some of their regular roles and responsibilities for a period of time. Selcom has focus on the following disasters

- *One or more vital systems are non-functional*
- *The building is not accessible due to technical issues and thus creates a failure to manage Server Room*
- *Failure of Single or Multiple IT Systems.*

The following events can result in a disaster, requiring this Disaster Recovery document to be activated:

- *Fire*
- *Pandemic*
- *Power Outage*
- *War*
- *Theft*
- *Terrorist Attack*

### Purpose

The purpose of this document is to capture all information regarding technical network structure and services that Selcom provides and secondly to implement and list down steps that will be taken during a disaster.

After all individuals have been brought to safety, the next goal of Selcom will be to enact the steps outlined in this DRP to bring all of the organization's groups and departments back to business-as-usual as quickly as possible. This includes:

- *Preventing the loss of the organization's resources such as hardware, data and physical IT assets*
- *Minimizing downtime related to IT*
- *Keeping the business running in the event of a disaster*

### Scope

**Selcom** takes all of the following areas into consideration:

- *Network Infrastructure*
- *Servers Infrastructure*
- *Telephony System*
- *Data Storage and Backup Systems*
- *Data Output Devices*
- *End-user Computers*
- *Database Systems*
- *IT Documentation*

This DRP does not take into consideration any non-IT, personnel, Human Resources and real estate related disasters. For any disasters that are not addressed in this document, please refer to the business continuity plan.



## **2. Disaster Recovery Teams & Responsibilities**

In the event of a disaster, different groups will be required to assist the IT department in their effort to restore normal functionality to the employees of Selcom. The different groups and their responsibilities are as follows:

- *Disaster Recovery Lead(s)*
- *Network Team*
- *Applications Team*
- *Operations Team*
- *Senior Management Team*
- *Communications Team*

The lists of roles and responsibilities in this section have been created by Disaster Recovery Team members who will be responsible for performing all of the tasks below. In some disaster situations, Disaster Recovery Team members will be called upon to perform tasks not described in this section.



## Disaster Recovery Lead

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs at Selcom, regardless of their department and existing managers. All efforts will be made to ensure that this person be separate from the rest of the disaster management teams to keep his/her decisions unbiased; the Disaster Recovery Lead will not be a member of other Disaster Recovery groups in Selcom

## Role and Responsibilities

- *Make the determination that a disaster has occurred and trigger the DRP and related processes.*
- *Initiate the DR Call Tree.*
- *Be the single point of contact for and oversee all of the DR Teams.*
- *Organize and chair regular meetings of the DR Team leads throughout the disaster.*
- *Present to the Management Team on the state of the disaster and the decisions that need to be made.*
- *Organize, supervise and manage all DRP test and author all DRP updates.*

## Contact Information

<b>Name</b>	<b>Role/Title</b>	<b>Mobile Number</b>
Mohammedjawaad Kassam	Primary Disaster Lead	+255784238772
Viola Urasa	Secondary Disaster Lead	+255743951550

## Network IT Team

### Mandatory

The Network Team will be responsible for assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the enterprise as well as telephony and data connections with the outside world. They will be primarily responsible for providing baseline network functionality and may assist other IT DR Teams as required.

### Role & Responsibilities

- *In the event of a disaster that does not require migration to standby facilities, the team will determine which network services are not functioning at the primary facility*
- *If multiple network services are impacted, the team will prioritize the recovery of services in the manner and order that has the least business impact.*
- *If network services are provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.*
- *In the event of a disaster that does require migration to standby facilities the team will ensure that all network services are brought online at the secondary facility*
- *Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order:*
  - *All members of the DR Teams*
  - *All C-level and Executive Staff*
  - *All IT employees*
  - *All remaining employees*
- *Install and implement any tools, hardware, software and systems required in the standby facility*
- *Install and implement any tools, hardware, software and systems required in the primary facility*
- *After Selcom is back to business as usual, this team will summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

### Contact Information

Name	Role/Title	Mobile Number
Rosario Arun George	HO of Technology and Software development	+255682852526
Mohammedjawaad Kassam	IT Compliance Officer	+255784238772

## Applications Team

### Mandatory

The Applications Team will be responsible for ensuring that all enterprise applications operates as required to meet business objectives in the event of and during a disaster. They will be primarily responsible for ensuring and validating appropriate application performance and may assist other IT DR Teams as required.

### Role & Responsibilities

- *In the event of a disaster that does not require migration to standby facilities, the team will determine which applications are not functioning at the primary facility*
- *If multiple applications are impacted, the team will prioritize the recovery of applications in the manner and order that has the least business impact. Recovery will include the following tasks:*
  - *Assess the impact to application processes*
  - *Restart applications as required*
  - *Patch, recode or rewrite applications as required*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with application patches*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with data copies*
- *Install and implement any tools, software and patches required in the standby acility*
- *Install and implement any tools, software and patches required in the primary facility*
- *After Selcom is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

### Contact Information

Name	Role/Title	Mobile Number
Rosario Arun George	HO of Technology and Software development	+255682852526
Mohammedjawaad Kassam	Application Manager	+255784238772



## Operations Team

This team's primary goal will be to provide employees with the tools they need to perform their roles as quickly and efficiently as possible. They will need to provision all Selcom employees in the standby facility and those working from home with the tools that their specific role requires.

### Role & Responsibilities

- *Maintain lists of all essential supplies that will be required in the event of a disaster*
- *Ensure that these supplies are provisioned appropriately in the event of a disaster*
- *Ensure sufficient spare computers and laptops are on hand so that work is not significantly disrupted in a disaster*
- *Ensure that spare computers and laptops have the required software and patches*
- *Ensure sufficient computer and laptop related supplies such as cables, wireless cards, laptop locks, mice, printers and docking stations are on hand so that work is not significantly disrupted in a disaster*
- *Ensure that all employees that require access to a computer/laptop and other related supplies are provisioned in an appropriate timeframe*
- *If insufficient computers/laptops or related supplies are not available the team will prioritize distribution in the manner and order that has the least business impact*
- *This team will be required to maintain a log of where all of the supplies and equipment were used*
- *After Selcom is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

### Contact Information

<b>Name</b>	<b>Role/Title</b>	<b>Mobile Number</b>
Sarah Mohamed	Chief of Operations	+255759617814
Navo Mshana	HR/Administrative Officer	+255754881079





## Senior Management Team

### Mandatory

The Senior Management Team will make any business decisions that are out of scope for the Disaster Recovery Lead. Decisions such as constructing a new data center, relocating the primary site etc. should be made by the Senior Management Team. The Disaster Recovery Lead will ultimately report to this team.

### Role & Responsibilities

- *Ensure that the Disaster Recovery Team Lead is held accountable for his/her role*
- *Assist the Disaster Recovery Team Lead in his/her role as required*
- *Make decisions that will impact the company. This can include decisions concerning:*
  - *Rebuilding of the primary facilities*
  - *Rebuilding of data centers*
  - *Significant hardware and software investments and upgrades*
  - *Other financial and business decisions*

### Contact Information

<b>Name</b>	<b>Role/Title</b>	<b>Mobile Phone Number</b>
Sameer Hirji	CEO	+25578645554
Sarah Mohammed	Chief of Operations	+255759617814



## Disaster Recovery Call Tree

In a disaster recovery or business continuity emergency, time is of the essence so Selcom will make use of a Call Tree to ensure that appropriate individuals are contacted in a timely manner.

- The Disaster Recovery Team Lead calls all Senior Staff and Head of department
- HOD will communicate to all individual staff in respective departments
- In the event staff is not available, deputy staff takes in charge of the responsibility

### 3. Recovery Facilities

In order to ensure that Selcom is able to withstand a significant outage caused by a disaster, it has provisioned separate dedicated standby facilities. This section of this document describes those facilities and includes operational information should those facilities have to be used.

#### Description of Recovery Facilities

The Standby facility will be used after the Disaster Recovery Lead has declared that a disaster has occurred. This location is a separate location to the primary facility. The current facility, located at <<Address of Standby Facility>> is 7.2kms away from the primary facility.

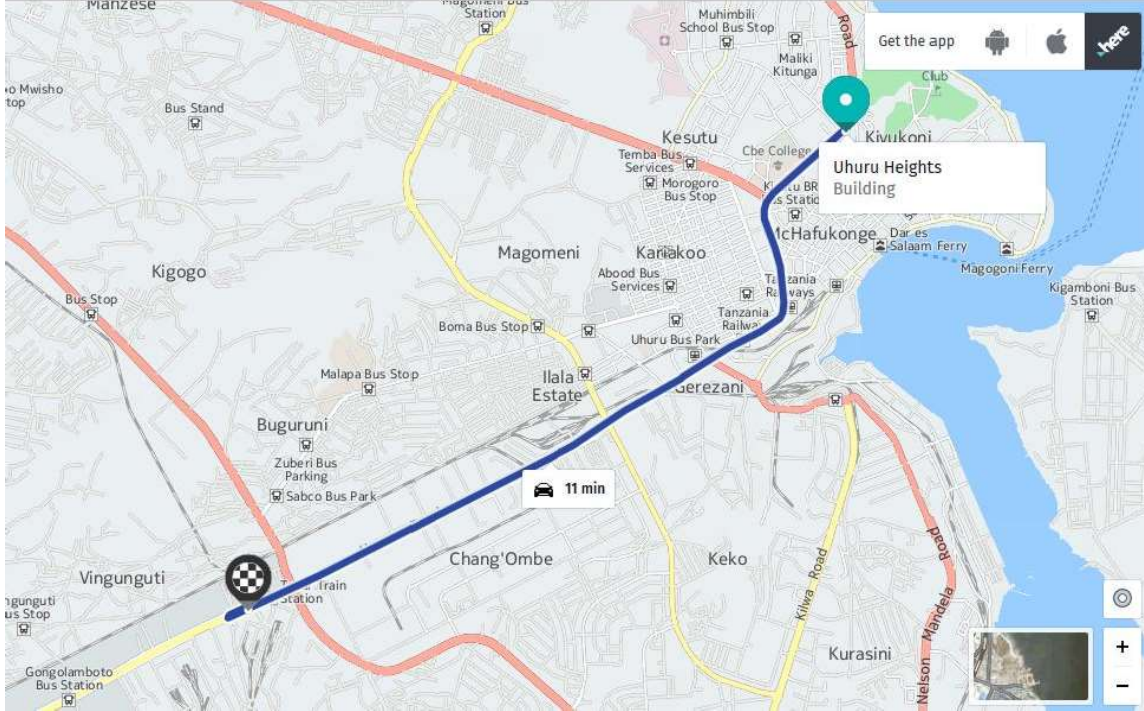
The standby facility will be used by the IT department and the Disaster Recovery teams; it will function as a central location where all decisions during the disaster will be made. It will also function as a communications hub for Selcom.

The standby facility must always have the following resources available:

- *Copies of this DRP document*
- *Fully redundant server room*
- *Sufficient servers and storage infrastructure to support enterprise business operations*
- *Office space for DR teams and IT to use in the event of a disaster*
- *External data and voice connectivity*
- *Sleeping quarters for employees that may need to work multiple shifts*
- *Kitchen facilities (including food, kitchen supplies and appliances)*
- *Bathroom facilities (Including toilets, showers, sinks and appropriate supplies)*
- *Parking spaces for employee vehicles*

## Directions to Recovery Facility

Under BCP the LTT Team will be responsible to manage Logistics during Disaster






### **Operational Considerations**

If employees are required to stay at the Standby Facility for extended periods of time and require hotel accommodations, they will be provided by Selcom. The Facilities Team will be responsible for determining which employees require hotel accommodations and ensuring sufficient rooms are made available.

If employees are required to stay at the Standby Facility for extended periods of time and require food, it will be provided by Selcom. The Facilities Team will be responsible for determining which employees require food and ensuring sufficient is made available via groceries, restaurants or caterers as appropriate.

While in the Standby Facility, employees must work under appropriate, sanitary and safe conditions. The Facilities team will be responsible for ensuring that this facility is kept in proper working order.



## Data Backup and Storage

This section explains where all of the organization's data resides as well as where it is backed up to. Use this information to locate and restore data in the event of a disaster.

### Data in Order of Criticality

Rank	Data	Data Type	Back-up Frequency	Backup Location(s)
1	Company Financial Documents	Confidential: Hard Copies	Scanned Documents	SAFE Cabinets
2	Company Financials on Software	Software	Daily	DR Site Storage Rack
3	Network Devices Backup and Log	Software	Daily Backup's for Logs and Monthly Backups for network Devices Snapshot	DR Site Storage Rack
4	Data Backups	Software	Daily Backup's for Data and Monthly Backups for entire Snapshot	DR Site Storage Rack
5	User Data Files	Confidential: Hard Copies	Scanned Documents	SAFE Cabinets
6	CCTV Backups	Software	Daily backup's on Same Location and Weekly backup on DR	DR Site Storage Rack
7	Vendor Data	Soft and Hard Copies	Daily backup's on Same Location and Weekly backup on DR and Scanned Copies	DR Site Storage Rack SAFE Cabinets



#### **4. Communicating During a Disaster**

In the event of a disaster Selcom will need to communicate with various parties to inform them of the effects on the business, surrounding areas and timelines. The Communications Team will be responsible for contacting all of Selcom's stakeholders.

##### **Communicating with the Authorities including regulatory reporting**

The Communications Team's first priority will be to ensure that the appropriate authorities have been notified of the disaster, providing the following information:

- *The location of the disaster*
- *The nature of the disaster*
- *The magnitude of the disaster*
- *The impact of the disaster*
- *Assistance required in overcoming the disaster*
- *Anticipated timelines*

##### **Authorities Contacts; Refer to BCP Documentation**

##### **Communicating with Employees**

The Communications Team's second priority will be to ensure that the entire company has been notified of the disaster. The best and/or most practical means of contacting all of the employees will be used with preference on the following methods (in order):

- *E-mail (via corporate e-mail where that system still functions)*
- *E-mail (via non-corporate or personal e-mail)*
- *Telephone to employee home phone number*
- *Telephone to employee mobile phone number*

The employees will need to be informed of the following:

- *Whether it is safe for them to come into the office*
- *Where they should go if they cannot come into the office*
- *Which services are still available to them*
- *Work expectations of them during the disaster*



## **Communicating with Vendors**

After all of the organization's employees have been informed of the disaster, the Communications Team will be responsible for informing vendors of the disaster and the impact that it will have on the following:

- *Adjustments to service requirements*
- *Adjustments to delivery locations*
- *Adjustments to contact information*
- *Anticipated timelines*

Crucial vendors will be made aware of the disaster situation first. Crucial vendors will be E-mailed first then called after to ensure that the message has been delivered. All other vendors will be contacted only after all crucial vendors have been contacted.

Vendors encompass those organizations that provide everyday services to the enterprise, but also the hardware and software companies that supply the IT department. The Communications Team will act as a go-between between the DR Team leads and vendor contacts should additional IT infrastructure be required.

**Crucial Vendors: Refer to BCP Documentation**



## 5. Dealing with a Disaster

If a disaster occurs in Selcom, the first priority is to ensure that all employees are safe and accounted for. After this, steps must be taken to mitigate any further damage to the facility and to reduce the impact of the disaster to the organization.

Regardless of the category that the disaster falls into, dealing with a disaster can be broken down into the following steps:

- 1) Disaster identification and declaration
- 2) DRP activation
- 3) Communicating the disaster
- 4) Assessment of current and prevention of further damage
- 5) Standby facility activation
- 6) Establish IT operations
- 7) Repair and rebuilding of primary facility

### Disaster Identification and Declaration

Since it is almost impossible to predict when and how a disaster might occur, Selcom must be prepared to find out about disasters from a variety of possible avenues. These can include:

- *First hand observation*
- *System Alarms and Network Monitors*
- *Environmental and Security Alarms in the Primary Facility*
- *Security staff*
- *Facilities staff*
- *End users*
- *3rd Party Vendors*
- *Media reports*

Once the Disaster Recovery Lead has determined that a disaster had occurred, s/he must officially declare that the company is in an official state of disaster. It is during this phase that the Disaster Recovery Lead must ensure that anyone that was in the primary facility at the time of the disaster has been accounted for and evacuated safely.

While employees are being brought to safety, the Disaster Recovery Lead will instruct the Communications Team to begin contacting the Authorities and all employees not at the impacted facility that a disaster has occurred.





## **DRP Activation**

Once the Disaster Recovery Lead has formally declared that a disaster has occurred s/he will initiate the activation of the DRP by triggering the Disaster Recovery Call Tree. The following information will be provided in the calls that the Disaster Recovery Lead makes and should be passed during subsequent calls:

- *That a disaster has occurred*
- *The nature of the disaster (if known)*
- *The initial estimation of the magnitude of the disaster (if known)*
- *The initial estimation of the impact of the disaster (if known)*
- *The initial estimation of the expected duration of the disaster (if known)*
- *Actions that have been taken to this point*
- *Actions that are to be taken prior to the meeting of Disaster Recovery Team Leads*
- *Scheduled meeting place for the meeting of Disaster Recovery Team Leads*
- *Scheduled meeting time for the meeting of Disaster Recovery Team Leads*
- *Any other pertinent information*

If the Disaster Recovery Lead is unavailable to trigger the Disaster Recovery Call Tree, that responsibility shall fall to the Disaster Management Team Lead

## **Assessment of Current and Prevention of Further Damage**

Before any employees from Selcomcan enter the primary facility after a disaster, appropriate authorities must first ensure that the premises are safe to enter.

The first team that will be allowed to examine the primary facilities once it has been deemed safe to do so will be the Facilities Team. Once the Facilities Team has completed an examination of the building and submitted its report to the Disaster Recovery Lead, the Disaster Management, Networks, Servers, and Operations Teams will be allowed to examine the building. All teams will be required to create an initial report on the damage and provide this to the Disaster Recovery Lead within <<state timeframe>> of the initial disaster.

During each team's review of their relevant areas, they must assess any areas where further damage can be prevented and take the necessary means to protect Selcom's assets. Any necessary repairs or preventative measures must be taken to protect the facilities; these costs must first be approved by the Disaster Recovery Team Lead.




## **Standby Facility Activation**

The Standby Facility will be formally activated when the Disaster Recovery Lead determines that the nature of the disaster is such that the primary facility is no longer sufficiently functional or operational to sustain normal business operations.

Once this determination has been made, the Facilities Team will be commissioned to bring the Standby Facility to functional status after which the Disaster Recovery Lead will convene a meeting of the various Disaster Recovery Team Leads at the Standby Facility to assess next steps. These next steps will include:

1. *Determination of impacted systems*
2. *Criticality ranking of impacted systems*
3. *Recovery measures required for high criticality systems*
4. *Assignment of responsibilities for high criticality systems*
5. *Schedule for recovery of high criticality systems*
6. *Recovery measures required for medium criticality systems*
7. *Assignment of responsibilities for medium criticality systems*
8. *Schedule for recovery of medium criticality systems*
9. *Recovery measures required for low criticality systems*
10. *Assignment of responsibilities for recovery of low criticality systems*
11. *Schedule for recovery of low criticality systems*
12. *Determination of facilities tasks outstanding/required at Standby Facility*
13. *Determination of operations tasks outstanding/required at Standby Facility*
14. *Determination of communications tasks outstanding/required at Standby Facility*
15. *Determination of facilities tasks outstanding/required at Primary Facility*
16. *Determination of other tasks outstanding/required at Primary Facility*
17. *Determination of further actions to be taken*

During Standby Facility activation, the Facilities, Networks, Servers, Applications, and Operations teams will need to ensure that their responsibilities, as described in the “Disaster Recovery Teams and Responsibilities” section of this document are carried out quickly and efficiently so as not to negatively impact the other teams.



## **6. Testing & Maintenance**

While efforts will be made initially to construct this DRP in as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the enterprise will change. As a result of these two factors this plan will need to be tested on a periodic basis to discover errors and omissions and will need to be maintained to address them.

### **Maintenance**

The DRP will be updated any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

- 7. Ensuring that call trees are up to date*
- 8. Ensuring that all team lists are up to date*
- 9. Reviewing the plan to ensure that all of the instructions are still relevant to the organization*
- 10. Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals*
- 11. Ensuring that the plan meets any requirements specified in new laws*
- 12. Other organizational specific maintenance goals*

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the company, it is the responsibility of the Disaster Recovery Lead to appoint a new team member.

## Testing

Selcom is committed to ensuring that this DRP is functional. The DRP should be tested every six months in order to ensure that it is still effective. Testing the plan will be carried out as follows:

- 1) **Walkthroughs-** Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DRP project manager to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities (if required).
- 2) **Simulations-** A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. However, validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.
- 3) **Parallel Testing-** A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.

Any gaps in the DRP that are discovered during the testing phase will be addressed by the Disaster Recovery Lead as well as any resources that will be required.

### 13. Document Control

Date	Version	Requester	Tech. Writer	Change/Review
21-06-2017	V1.0	Sameer Hirji	Mohammedjawaad Kassam	Sarah Mohamed
30--08-2017	V1.1	Deloitte/SCB	Mohammedjawaad Kassam <i>- Section 4 of the documented Updated with SCB Server will not have access to remote printing- Disabled</i>	Sarah Mohamed
17-10-2017	V1.1	Internal Change	Mohammedjawaad Kassam Update HR Staff	Sarah Mohamed
19-09-2023	V1.2	InternalChange	Viola Urasa Updated Staff list	Mohammedjawaad Kassam