
# Data Security and Protection Policy

Connect Mobile Communication - 2019/2020

## Review and Update

This document will be reviewed annually, due to continuous changes, evolving communities and developing organisational data security and protection policies. This document will be audited by a third party every four years or as and when required by law and/or regulatory changes or amendments.

## Document Custodian

It is expected that the custodian of this document is every stakeholder associated with this company “Connect Mobile Communications”. The entity as custodian is the Executive Management Division, and any comments or proposed changes should be communicated through them.

## Policy Compliance and Verification

Executive Management as authorised security and information officers will verify compliance to the below mentioned policies through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits and feedback from all clients and/or employees. Any exception to the policy must be approved by the Executive Management in advance.

Any exception to the policy must be approved by the senior management in advance.

An employee found to have violated any of these policies may be subject to disciplinary action, up to and including termination of employment.

## Document History

| **Revision** | **Date** | **Author** | **Change Description** |
|---|---|---|---|
| Draft 1 | June 2019 | Doug Jenkinson | First draft for internal review. |
| Final Version 1 | Sept 2019 | Doug Jenkinson | Revisions based on feedback. Finalised. |

# Table of Contents

# Introduction

In the past, the approach to data protection and security has boiled down to efforts to simply secure the infrastructure in which the data resides and flows. In recent times it has become obvious that it is far more difficult to build protection around infrastructure where the perimeter is far more fluid in a world of cloud computing and mobile devices.

For this reason, our approach to securing and protecting our data and that of our partners is focussed on guarding the data itself. While typical infrastructure protections will always be employed as a second layer of protection, our primary security comes in the form of process and protocol surrounding how our data is handled, accessed and processed.

To achieve this continued level of security on the data itself, we need to continually focus on the following criteria:

- Clear and well defined goals
- Data classification
- Safe and compliant data retention policies
- Data protection technology
- Establish auditing and impact assessment protocols
- Establish a list of approved business software
- Employee policies and protocols for securing and handling data
- Incident detection
- Incident response
- Training

# Goals

The following is a list of goals that this document is designed to achieve through policy and protocols are to:

- Adhere to regulatory requirements and contractual agreements in terms of the protection of sensitive, private and confidential data in the regions in which we operate.

- Protect the privacy of clients and our clients customers.
- Prevent loss, harm or damage, whether personal or business related, to clients or our clients customers through the compromise or loss of sensitive data.
- Guard Connect Mobile, its clients, and its employees from legal, ethical or contractual breaches that may result from the compromise or loss of sensitive data.
- Ensure that we anonymise or destroy sensitive or private data that is of no operational or business use.
- Ensure our employees are fully informed on why data protection is important, and continuously educate them on approved software and protocols.

## Data Scope

As an IT/Telecommunications company, our data and information has many forms and resides in many different locations. Below is a short definition of the type of data that we store and where it is located.

- Physical documents and contracts (filed away securely on-site)
- Digital documents, spreadsheets and contracts (G-Suite, Office 365, also stored on employee computers)
- Email (Gmail via G-Suite)
- Chat messages and notifications (Telegram)
- Photographic or video content (GDrive via G-Suite, some data stored on local employee computers)
- Digital Databases (stored in a data centre, some data on-site)
- Transaction logs (stored in a data centre, some data on-site)
- Source Code (stored in a data centre, some data on-site)

# Data Classification

In order to implement protections around company, client and supplier data, we need to define different classes of data, from which we can apply rules and varying protection processes on each classification as required.

These classifications are:

- **Public Data**
  This definition encompasses all information and data that are available in the public domain. These include:
    - Marketing material
    - Integration documents, guides and instruction manuals
    - Service offerings and generic price lists
    - Public notifications and announcements
    - All content contained on publicly accessible portions of the company website
    - All content published on social media platforms
    - All published photographic or media content
- **Internal Data**
  This definition encompasses any data or information that is created by the company or handed to the company by clients during the normal course of business, which would not be classified as confidential or restricted. A leak of this data is not considered a threat, but it should not be publicly exposed. These include:
    - Email or logged telephonic correspondence with clients where no sensitive or personal information is discussed or shared.
- **Confidential Data**
  This definition encompasses all internal information created or given to the company that is bound by contractual confidentiality. It also encompasses any information or data that may cause financial, legal or reputational damage to Connect Mobile or it's clients or suppliers if leaked or shared with unauthorised persons and/or organisations. These include:
    - Client and supplier data, such as
        - Customer information
        - Transactional or user logs
        - Usage, Sessions or SMS statistics.

        - Reports of any kind
        - Financial, billing data and invoices
    - Product development plans or documentation (IP owned by ‘The Company’)
    - Unpublished photographic or video content, usually related to marketing
    - Technical plans or documentation (IP owned by ‘The Company’)
    - Network system architecture documentation or diagrams (IP owned by ‘The Company’)
    - Internal developer documentation (IP owned by ‘The Company’)
    - Internal process and operational documentation (IP owned by ‘The Company’)

      *** General Note (Any of the above mentioned - “Anything that is planned, designed, created, developed, documented by any individual/employee within ‘The Company’s operating hours, on the premises after hours, using any resources of ‘The Company’ will by Law be “IP owned by ‘The Company).

- **Restricted Data**
  This definition encompasses all internal data or information that belongs to Connect Mobile that must be strictly access controlled for legal/regulatory compliance, contractual or security reasons.
    - Client and supplier lists
    - Client and supplier contracts and agreements
    - Client and supplier pricing
    - Employee personal information
    - Employee contracts, agreements, remuneration and benefits
    - Company financial reports
    - All account passwords
    - Legal documents

# Data Roles and Responsibilities

It is important to understand the roles and responsibilities of different employees in different departments in terms of access to, and responsibility for, different types of data in the company.

It should be noted that the data and information listed here will only be accessed by the mentioned parties when it is absolutely necessary for operational, service or support reasons.

- Client Support
  Client support representatives handle the day to day communication via phone and email. They will attempt to assist clients in all queries and needs regarding company service, as such, they have access to and are responsible for:
    - Email correspondence(customer, support)
    - Client payment and invoice requests
    - Client files and data
    - Client reports, on occasion
- Operations Department
  The operations team handles more complicated service requests as well as internal operational data of the company.
    - Email correspondence (customer, support, operations)
    - Client Data
    - Client Reports
    - Partner/supplier data
    - Contracts (restricted access)
- Routing Department
  Routing department handles all SMS routing, as well as client support issues on a technical level. This job requires access to confidential and restricted data for senior employees in the department.
    - Email correspondence (customer, support, operations, suppliers, routing, client finance)
    - Client Data
    - Client Reports

    - Company Databases (restricted access)
    - Contracts + pricing
    - Supplier data

- Finance Department
  The finance department handles typical sets of data for a finance department in any company, which includes sensitive, restricted and confidential data.
    - Email correspondence (customer, client finance)
    - Client reports, stats
    - Client invoices
    - Employee contracts and payslips
    - Company financial documents, statements
    - Credentials to third party financial systems (which should be properly secured).

- Development Department
  The development department has the most access to technical data within the company in order to perform their function. This requires development specific controls and protocols for how data is handled in this context.
    - Database access (restricted by need to know)
    - Source Code
    - Administrative and client reports
    - User/Service/Client accounts
    - Architectural and design documentation
    - Employee email accounts and activity (restricted to certain developers)

- Executive Management
  Management requires access to almost all data and information in the company, but this data and information (particularly sensitive, confidential and restricted) can only be accessed when it is critically needed.
    - Client, partner and supplier data
    - Financial reports
    - All contracts and legal documents
    - Employee records and contracts

- Secure encryption keys (where applicable)

# Data Retention Policy

While a good data retention policy plays an important part of compliance, it also plays a part as a defense against security breaches by not holding onto any sensitive data longer than is required. We have agreed to the following protocols regarding the storage and retention of sensitive data, which are in line with protocols outlined by common legislation such as the European GDPR or South African POPI acts.

Google G-Suite provides a set of tools that are used to enforce retention policies, particularly for legal and compliance purposes.

1. Client/Supplier Data

    1.1. Connect Mobile will not hold onto any client or supplier data for longer than is required in order to provide optimal service.

    1.2. All private information relating to any persons, be it customers, partners, or employees, contained within client data (SMS Traffic, USSD sessions) must be anonymised or destroyed as soon as it is no longer required for support or service reasons.

    1.3. The default time period for raw data retention is three months for reporting and recon purposes.

    1.4. Any data that is confidential or restricted that needs to be preserved unchanged for longer than is needed for the company to provide its services, be it for contractual or legal reasons, must be archived, encrypted and stored in a secure, access controlled location.

    1.5. All data stored offsite (such as on AWS Glacier) must be stored in an encrypted format and strictly access controlled.

    1.6. Connect Mobile will not store any personal or confidential client or supplier information, particularly the personal information of their employees, for any period of time if such data is not required for operational or contractual reasons.

    1.7. Records of trade with clients or business entities will be stored securely in perpetuity. This does not include any personal information.

    1.8. Connect Mobile will hand over or destroy any client data on request from the client, provided proper identification and permission is provided by a client representative.

2. Company Documents and Contracts

    2.1. Confidential and restricted digital documents will be stored in the G-Suite Drive in strictly access controlled folders, and deleted when no longer needed.

    2.2. Physical documents of the same classifications will be filed away in locked storage units, and destroyed when no longer needed.

3. Employee Private Data

    3.1. Connect Mobile will not hold onto private employee information for longer than the employment/contract period of the employee, unless such information must be preserved as required by law, or is needed to contact the employee after employment has ended at the company.

    3.2. A record of an employee's employment at Connect Mobile will be kept in perpetuity.

    3.3. Employee information to be securely preserved after employment will be:

        3.3.1. Name and Surname

        3.3.2. Phone Number

        3.3.3. Last Known Address

        3.3.4. Employment Contracts

        3.3.5. All Payslips and Financial records relating to remuneration and benefits

        3.3.6. All records of attendance

        3.3.7. All prior internal or external communication using company accounts

        3.3.8. All written general or disciplinary notices

# Employee Guidelines

People play one of the largest and most important roles when it comes to data security in an organisation, since the people within the organisation are closest to critical information and in some instances hold most of the keys to accessing that information.

Below represents a set of policy guidelines that all employees must read, understand and adhere to. Training must be provided for all current employees and new hires on the information below (and listed throughout this document)

# Business Software

Connect Mobile has a set of approved software and web services that can be used for general business and operational needs. It is important that every employee only uses approved software, and follows both general and specific guidelines regarding the use of such software in order to protect confidential information and private data.

The following is a list of the approved software and their appropriate uses.

All software must be kept up to date with the latest available versions where applicable.

1. Google G-Suite
   With all usage limited to the accounts created for employees by the administrative teams. Never login or use personal Gmail accounts when using this software for any of the following business reasons.

   1.1. Email (Gmail)

   1.2. Events, bookings and meetings (Google Calendar)

   1.3. Chat services (Google Hangouts)

   1.4. File and document storage (Google Docs, Google Drive)

   1.5. Document creation and editing (Google Docs, Google Drive)

2. Plugin
   Plugin is Connect Mobile's internal web platform, used for client self service and administrative tasks.

   2.1. Account, service and routing management

   2.2. SMS Management and Sending

   2.3. USSD Management

   2.4. Reporting

   2.5. Contact Management

   2.6. System Configuration

3. Telegram
   Telegram is used internally for communication and coordination amongst staff, as well as notifications. All messages on Telegram are restricted to non-confidential conversations and information.

   3.1. Business discussion

3.2. Planning and coordination

3.3. Casual banter

3.4. System notifications

4. Sage
   Highly restricted and access controlled accounting software.

5. Pipedrive
   Sales management software. (CRM)

6. Active Campaign
   Web based marketing automation platform.

7. Microsoft Office 360
   Alternative for Google Docs on G-Suite, Microsoft Office applications should only be used in cases where Google Docs does not suffice for the management of client documents, spreadsheets and presentations.

8. Last Pass
   Password management tool, see Password Protocols below.

9. Toggl
   Web based time tracking software.

10. Jira
    Web based project management software geared towards software development. Jira boards, files and tasks should be adequately restricted and access controlled.

11. Trello
    Web based project management software, for general project management and planning purposes.

12. Skype
    Skype is used to communicate with certain clients/suppliers where Skype forms part of their own business communication process. Skype must not be used for internal communication.

13. Google Hangouts
    Google Hangouts is used to communicate with certain clients/suppliers where Hangouts forms part of their own business communication process. Hangouts can be used for internal communication provided the user is logged into their work email account.

14. WhatsApp
    WhatsApp is used to communicate with certain clients/suppliers where WhatsApp forms part of their own business communication process. WhatsApp must not be used for internal communication, with the exception of testing certain services.

15. Facebook
    Facebook is used to interact with Connect Mobile's social media community. No personal or sensitive data must be shared on this platform.

16. LinkedIn
    LinkedIn is used to interact with Connect Mobile's social media community. No personal or sensitive data must be shared on this platform.

17. Twitter
    Twitter is used to interact with Connect Mobile's social media community. No personal or sensitive data must be shared on this platform.

18. Approved Browsers
    Connect Mobile does not have a particular requirement for web browsers. The following are acceptable as long as the browsers are kept up to date and password remember functions are not used.

    18.1. Google Chrome

    18.2. Microsoft Edge (IE is not to be used except for software testing)

    18.3. Mozilla Firefox

    18.4. Opera

    18.5. Apple Safari

# Password Protocols

Strong passwords are a vital first line of defense when it comes to digital security. Listed below are guidelines for password creation and usage. Lost, stolen or easy to guess passwords can cause significant damage or loss for the company, so adherence to this policy is vitally important.

1. Password Creation Guidelines

    1.1. Passwords should be auto generated using the LastPass password management service to ensure long, secure passwords.

    1.2. In cases where LastPass cannot be used:

        1.2.1. Passwords should be 8 characters or more.

        1.2.2. Passwords should not contain any personal information, such as names, addresses, phone numbers, birthdays, or names of obvious interests.

1.2.3. Passwords should not contain any number or keyboard patterns such as “12345” or “qwerty”.

1.2.4. Passwords must not be any form or variation of common passwords https://en.wikipedia.org/wiki/List_of_the_most_common_passwords https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt

2. Account Password Guidelines

2.1. Users must use a separate unique password for each individual work account. LastPass will enforce this.

2.2. Never use work passwords for personal accounts, or vice versa.

2.3. Users must make use of 2FA (two factor authentication) for any account on any service that supports such a security feature. 2FA usually takes the form of an SMS or email that is used to confirm the identity and session of a user on a particular device after typing in a password.

3. Password Changes

3.1. Passwords should be changed when there is reason to believe that a password has been compromised.

3.2. Password cracking or guessing can be done at any time by our internal security team or contracted external security testers. If a password is guessed or cracked, the user will be required to change it immediately.

4. Password Protection

4.1. All passwords are to be treated as restricted and confidential information of Connect Mobile.

4.2. Passwords must never be shared with anyone internally or externally, this includes colleagues, supervisors, clients or suppliers.

4.3. Raw passwords must never be inserted in emails, SMS messages, Telegram/WhatsApp messages, or any other chat or communication system, with the exception of client passwords on Plugin. A process on Plugin will be established to automate administrative password resets.

4.4. Passwords can be stored in our approved password manager LastPass - https://www.lastpass.com/

4.5. Avoid using “Remember Password” features of any application, including the users web browser.

4.6. Any user that suspects that their password has been compromised must immediately report it to the devops team and change all passwords.

5. Software Development Password Guidelines

5.1. Database and account credentials (particularly passwords) should not be stored in plain text in any source code.

5.2. Passwords and sensitive credentials should be stored in a centralised and protected repository managed by the DevOps team.

5.3. All passwords must never be transmitted across the network in pure form.

5.4. All applications must have a separate credential set for each database or account/service used by each application. No application should share similar credentials.

# Email

Email forms the primary basis of internal and external communication for the company. Not only is email ubiquitous, it plays a strong role in establishing a paper trail and history of communication with clients and suppliers. A consequence of this is that a considerable amount of private or confidential information is passed around via email, therefore strict procedures must be followed in order to secure our data and that of our partners.

1. Email Accounts

1.1. All company email accounts must be created and managed using Connect Mobile's Google G-Suite. No other external or 3rd party email accounts can be used for any business communication whatsoever.

1.2. Employee email accounts are considered restricted and confidential for each employee. Therefore no employee may attempt to access or read email on another employee's account.

1.3. Management reserves the right to access and monitor all email on all email accounts within the organisation.

1.4. No communication via Connect Mobile email accounts can be considered private for any employee.

2. Email Conduct and Usage

2.1. Company email should be used for business related communication only. Personal communication is permitted on a limited basis, but no non commercial communication is allowed.

2.2. Do not use company email accounts to register or create accounts or services on 3rd party sites where the account is not for company use. Email accounts should not be linked to any personal accounts on platforms such as social media, online banking services, or any software service that is personal in nature.

2.3. All accounts created on any external websites, services or platforms using Connect Mobile email addresses are considered property of Connect Mobile.

2.4. All email messages must be consistent with applicable policies and procedures in terms of legal, ethical, safety and compliance with all applicable laws and contractual agreements.

2.5. Do not create, send or forward any email messages that are disruptive or offensive, such as messages containing offensive subject matter about race, gender, body appearance, disabilities, age, sexual orientation, pornography, religious beliefs, political beliefs or national origin. Employees who receive email containing any of the above mentioned content should report it to management immediately.

2.6. All confidential or restricted data and attachments contained within any email must be secured by encryption or password protection. Using the G-Suite Drive to share locked files is advised in all cases over sending of attachments.

2.7. As part of the password policy, do not share passwords via email. If a password is shared via email, the recipient is required to immediately change the password for the related account.

2.8. Forwarding email to outside addresses that are not related to Connect Mobile or the confidential subjects discussed in the email in question is prohibited.

2.9. Automatically forwarding emails to a third party or external accounts is prohibited. Employees may only use their main business email account to read and send emails.

2.10. Any employee who accidentally or intentionally receives any email relating to confidential or restricted information clearly not meant for their eyes, regarding company operations, client or supplier agreements, or anything relating to confidential information about the company, another employee or any person whatsoever, is required to immediately report the breach to management.

# Telegram

Telegram is an integral chat service used for day to day operations and support discussions between employees, as well as system notifications and statistics. Due to the account portability and the many available clients on most operating systems, it is difficult to lock down Telegram, and as such, strict rules apply to what kind of data can be shared over Telegram.

1. Employee Chats

    1.1. Sharing of confidential or restricted information on Telegram groups or chats is strictly prohibited. Use email instead, and only share such information with the appropriate people.

    1.2. Uploading and sharing of sensitive documents or files that are not encrypted is strictly prohibited. Share files using access controlled G-Suite Drive instead, and ensure all files shared via Drive are not publicly available by restricting their access to the email addresses of those who require access.

    1.3. Do not send passwords or credentials over Telegram.

    1.4. All text messages must be consistent with applicable policies and procedures in terms of legal, ethical, safety and compliance with all applicable laws and contractual agreements.

    1.5. It is prohibited to send any messages to employees, clients or company groups that are disruptive or offensive, such as messages containing offensive subject matter about race, gender, body appearance, disabilities, age, sexual orientation, pornography, religious beliefs, political beliefs or national origin. Employees who receive messages containing any of the above mentioned content should report it to management immediately.

2. Business Groups

    2.1. Only employees who absolutely require access to and the information on specific groups should be included as members of such groups.

    2.2. All notification groups must be created and owned by a Connect Mobile phone number and not the private account of any employee.

    2.3. All business groups must be created, owned and administered by a senior manager or senior member of the development team.

3. Application and System Notifications

    3.1. It is prohibited to include any confidential, restricted or personal information about Connect Mobile, it’s clients, client customers, providers, partners or employees in any automated notification on any group.

3.2. Access to these notifications should be restricted to need to know employees only.

# Plugin

Plugin is Connect Mobiles proprietary administrative and client self service web system, which is available online through any web browser. Plugin acts as a gateway/online portal for employees and clients to access Connect Mobile's SMS and USSD functions and reporting. As a result, Plugin represents a potentially open line to a large amount of confidential and restricted information, especially for employees.

While a large effort has been made to secure data on Plugin, administrators still wield a huge amount of power within the system to view client data. As a consequence, it is vital that employees with administrative rights adhere to the following rules regarding access and data on Plugin.

1. Administrative Guidelines

1.1. Never download, reveal or share any confidential or restricted data to any client or third party outside of Connect Mobile or any unauthorised employees. These include:

1.1.1. MTSMS statistics

1.1.2. MOSMS statistics

1.1.3. Delivery statistics

1.1.4. USSD statistics

1.1.5. Client sending statistics or behaviour

1.1.6. User activity

1.1.7. MTSMS or MOSMS records, including mobile numbers or message content

1.1.8. USSD session data, including mobile numbers and user input

1.1.9. Client customer personal information of any kind, whether derived from contact lists or message content

1.1.10. Client lists or pricing

1.1.11. Provider lists or pricing

1.1.12. Financial data of any kind

1.1.13. Contact details or personal information of any user on Plugin

1.1.14. Reports of any kind unless that information pertains to a particular client request

1.2. Never share any passwords of any users on any platform whatsoever. If you must set a password on behalf of another user, use the proper process in order to ensure that a user changes the password on the next login.

1.3. Never add any users or create any accounts without express authorisation from management or the accounts department.

1.4. Never enable or disable a user or account without express authorisation from management or the accounts department.

1.5. Never view or attempt to access any client data that is not required for a support query or operational reason.

1.6. Never make any changes to a client user, account, service or data without permission from management and the client in question.

## G-Suite and Google Drive

G-Suite provides the company with excellent identity and rights management, access control and auditing alongside the easy accessibility to the system both on-site and off-site. It is important to restrict most document storage, collaboration and management to Google Drive within the company G-Suite account in order to get the most out of it's security benefits.

As a result, **all employees are required to store and document client data on Google Drive under their @connect-mobile.co.za account, using either their personal work drive or team drive**. Documents may not be stored in any other service or any other physical storage other than temporary use files on the employees local computer.

## Handling Client Files and Data

Clients and partners send us large amounts of documents and data files. At this point, it's a critical part of how we do business, but also exposes challenges in terms of protecting that data as it is passed around between internal employees (Connect Mobile Communication) and our external clients and partners.

While we have little control on how clients handle their data, we can apply best practice to protect this data on our side, the following are a set of strict rules that apply towards how this data is handled:

1. Store client data on G-Suite Google Drive only, not on local file systems, and not on any other service.
2. If client data must be downloaded onto your local computer in order to perform an action (such as a contact list import or bulk send), the client data must be immediately deleted after use.
3. As above, destroy any client data in long term storage (G-Drive) that is no longer needed.
4. If the file relates to a project plan or campaign plan, it must be immediately stored in the work account GDrive instead of downloading it.
5. Always share client data via secure (non-public) G-Drive links.
6. If a file needs to be shared via a public link, the file must be destroyed or the link disabled as soon as the client has confirmed receipt.
7. Only share client data with fellow employees if the employee in question requires access in order to do their job. Do not broadcast data to all employees.
8. Do not share client files and data via Telegram, WhatsApp, Skype or any other messaging or social media client with anyone.
9. Do not share client data with any organisation or third party outside of the company without express permission of management and authorised representatives of the client.
10. Do not attach or send client data or files in email unless the data needs to be delivered to an external recipient approved by the client as mentioned in point 8.
11. Downloading, transfer and removal of any client data is strictly prohibited. At no point must client data be stored on any physical storage medium such as a USB drive, mobile phone or computer other than your own for business purposes.

## Mobile Phones

Mobile phones and personal devices represent new challenges for organisational security due to their portability while being a critical productivity tool for most employees. Enforcing security rules and adhering to protocols when it comes to the usage of mobile devices will help minimise the risk of private and sensitive data being leaked outside the organisation.

All private devices that are utilised by employees using their work profile are required to adhere to the rules of the G-Suite device management plan. This is automatically enforced when any employee attempts to login to their device using their @connect-mobile.co.za address. These device policies enforce the following properties on a private device:

- An employee's device must be encrypted by default.
- All Google apps and services that work under the work profile are kept completely separate from personal apps and services on the device.
- Only Connect Mobile approved apps may be installed when using the work profile.
- No messages, files, images or screenshots can be shared between work profile apps and other private apps.
- The employees account can be remotely wiped. This function will only wipe data and apps related to the work profile, and leave personal data and apps intact.

## Access points and networking equipment

- No private access points or other networking equipment may be used on the premises without express permission from management
- Security between systems that need DC connectivity is strictly controlled using OpenVPN certificates. These certificates must be invalidated when a client leaves the company.

# Security Technology

## Identity and Access Management

Our IAM (Identity and Access Management) structure is currently fragmented, and split across several domains, depending on the services or technologies required for Connect Mobile to conduct its operations. A future update to centralise IAM is planned.

- G-Suite
  Employees are granted email accounts “@connect-mobile.co.za” in the company G-Suite domain that identify and control access to email, documents, events and other Google services for the company. Employees also use these email addresses to register on other third party web services on behalf of the company, in order to maintain company ownership over those accounts.
  For more information on the security tech provided by G-Suite, please visit the following link:
  https://gsuite.google.com/learn-more/security/security-whitepaper/page-9.html

- Plugin
  Employees and clients are issued with a Plugin specific user, which grants access to Connect Mobile SMS, USSD and reporting systems.
- AWS IAM
- Personal Accounts
  This covers things like Telegram accounts. These are managed by individual employees, and are granted access to certain company channels, such as Telegram groups. This is the weakest part of the IAM architecture, as there is no centralised way of identifying and controlling access for these accounts.
- Cacoo
- 3CX telephony
- Spanning backup (Comprehensive backup system for GSuite.)

## Enterprise Digital Rights Management (DRM)

Rights and access is explicitly controlled by Google G-Suite tools, which applies individual and group permissions to users who can access content within this ecosystem. Google uses what is called an IRM (Information Rights Management) to provide granular rights control on documents and other data within the G-Suite ecosystem.

Plugin features a rudimentary rights system, but is currently lacking with only two levels of rights management. A new permissions system has been partially built, but has not been completed by the time of writing.

Closer integration to the G-Suite accounts is desired on Plugin using G-Suites SSO (Single Sign On) integration.

It should be noted that Telegram is still lacking some sort of rights management other than access control via membership to certain groups.

## Data Loss Prevention (DLP)

G-Suite provides a powerful DLP (Data Loss Prevention), which allows administrators to set rules and keywords for detection in outgoing or incoming mail, and even apply automated rules to these messages, to either scrub, quarantine or block such messages.

These rules and keywords should be reviewed once a year and updated to protect against the latest anticipated angles of attack or leakage.

More on G-Suite DLP: https://support.google.com/a/answer/6280516?hl=en

Backups are run every day by the spanning backup system. Access is restricted to G-Suite administrators.

## Breach Detection

Breach detection covers a broad subject of monitoring our infrastructure and our data to detect intrusions. This subject is noted in minor detail, as implementation of our breach protection systems will be spearheaded after we conduct a Data Protection Impact Assessment (DPIA) and a proper security audit.

At this point, Google Vault provides tools to audit user activity with regards to documents and emails. This requires manual monitoring of activity.

G-Suite Drive Audit Log Alerts can notify admins of specific activity, such as documents being shared with the word “Confidential” in them, in order to detect breaches as they happen.
https://support.google.com/a/answer/4579696

We can look into introducing Breach Detection Tools that monitor network and user activity for anomalies within our network. The resolution of our breach protection systems will be resolved when we conduct a Data Protection Impact Assessment and Security Audit.

# Data Breach Incident Response

The following represents a basic set of steps to follow in the event that a data breach has been identified.

1. **Determine Loss**
   Determine what data was lost or compromised, and where it was stored.

2. **Secure and Lockdown**
   Change all passwords and lock down access to the data storage site until the breach point has been identified.

3. **Identify and Inform Parties**
   Immediately identify and inform all parties that are affected by the breach, such as clients, suppliers or employees. In the case of sensitive, restricted or confidential data, the related parties must be informed as soon as they have been identified. In the case of internal data loss that is not sensitive, clients can be informed as soon as the report is assembled in step 6. If passwords are affected, external parties must be instructed to change their passwords immediately.

4. **Determine Cause/Attack Vector**
   Determine how the breach took place, whether accidental or intentional. Identify weaknesses in process, security or software that allowed the breach to take place.

5. **Corrective Actions**
   Once the cause is identified, immediately take steps to patch the breach point and institute process/software to prevent a similar future breach.

6. **File a Report**
   Compile and store a full internal incident report on the breach. A redacted report (that excludes sensitive security information) can be assembled and provided to affected clients or partners.

# Employee Training

People are one of the most powerful weapons when it comes to data protection and security within an organisation. In order to wield this weapon, people in the organisation need to be properly trained on the reasons and protocols behind data security. Data protection and security is the responsibility of all people in our company.

All employees shall undergo data security training once a year, covering all the subjects mentioned in this document.

All new employees will undergo training as soon as their employment at Connect Mobile begins.