PASSWORD POLICY

1 PURPOSE OF DOCUMENT

The purpose of this document is to define and enforce a policy that will have a mitigating effect on the security risks associated with the internal management of Passwords.

2 SCOPE

The effect of this policy document is applicable to all RLM internal IT Systems and Infrastructure that have password-protected access.

3. AUDIENCE

This policy is applicable to:

- All RLM employees, contractors and agents who act on behalf of the RLM or are in its employment and are End Users of the RLM internal IT Systems and Infrastructure;
- All Business Units and Departments within the RLM as well as its affiliated entities of which the RLM has management control;
- All System Administrators appointed with administration responsibilities that are directly or indirectly governed by the specification contained in this policy.

4. RATIONALE

The internal IT Systems and Infrastructure are important assets to the business and disruption of their operation can have a negative impact on our business and clients. Such systems are under continual threat of events that can negatively affect them and consequently the business. The order of the impact and the likelihood of the event, constitute a so-called IT security risk. These risks can be mitigated or reduced by proactively instituting policies whereby the likelihood of occurrence and the order of impact is reduced to acceptable levels.

The IT Assets have been classified according the main IT architecture components and subcomponents. A list of potential and relevant security threats has been compiled and the likelihood of each determined. The Password mismanagement is a potential security threat. The process as defined in this policy document should be used as the de facto standard.

5.0 DEFINITIONS

AD	Active Directory
PC	Personal Computer
SMS	Short Message Service

Password	**A password** is a secret word or string of characters that is used for authentication, to prove identity or gain access to **a**
User-Id	Integer value called a **user identifier,** often abbreviated **to UID** or **User-ID**
Password Self-service reset	**Self-service Password Reset** is defined as any process technology that allows users who have either forgotten th password or triggered an intruder lockout to authentica with an alternate factor, and repair their own proble without calling the help desk.
Random Password Generator	A random password generator is a software program that takes input from a random or pseudo-random number generator and automaticall generates a password.

6 POLICY OBJECTIVES

The objectives of the RLM Password Policy are:

(a) Mitigation of risks associated with Password mismanagement;

(b) Enforce password standards; and

(c) Enforce a Password change procedure.

7. POLICY STATEMENT

7.1 User-id and password

- Access to all IT Systems and Infrastructure will be controlled by means of a user-id and password;
- The owner of a user-id and/or password is fully responsible to ensure that no other person can make use of it to access the IT Systems and Infrastructure;
- All user-id's and passwords shall be treated as Confidential and Organization sensitive information.
- All vendor supplied default or generic user-id's must be removed, renamed, disabled and/or passwords changed;
- End User accounts will be de-activated after a maximum of five (5) consecutive unsuccessful attempts to enter a password. This account will stay inactive for 30 minutes, or until a System Administrator has re-activated the account;
- It is mandatory that screen saver passwords be activated on PC's. Following no activity on a PC for a maximum of ten (10) minutes, the screen saver password must be

automatically invoked. For terminals, the system must automatically blank the screen and suspend the session after 10 minutes; wherever possible, applications should automatically invoke a session timeout after 10 minutes of inactivity. Re-establishment of the session must take place only after the End User has provided the proper password;

- It is mandatory that all PC's connected to the network be logged out of the network regularly. It is recommended that this be done each day; A forced logout from the network will be implemented to occur once a week at an appropriate time;
- All enterprise servers and network switching equipment must be password protected and where practically possible, adhere to all requirements stated in this policy.
- Where applicable all systems shall have the "Remember Password" option disabled e.g. Internet Explorer websites.

7.2 Password standards

- All passwords must have at least eight (8) characters;
- Passwords should not be a word found in the dictionary or some other part of speech. For example, proper names, places, and slang should not be used;
- Passwords should not contain other information easily obtained about you. For example, date of birth, license plate number, telephone number, ID number, make of your car, house address, etc.;
- Passwords should not be all digits nor should the password contain more than two of the same letter consecutively;
- Where the operating environment allows, passwords must contain a combination of at least three of following four classes:
    - English Upper Case Letters A, B, C, ...Z;
    - Westernized Arabic Numerals 0, 1, 2,... 9;
    - At least one special characters e.g. punctuation symbols !®,#$%A&*0+h-=Vf)n:":'<>?../
    - Passwords should be easy for the End User to remember, but not easy for someone else to guess. For example, the phrase "It's always your duty to stay

informed!" Might be the basis for a password such as Iayd2si! This password uses a mix of alphanumeric, and punctuation characters. A date could be added, e.g. January 2004 could be represented by 01-04, or even)! -)$ (By making use of the shift key);

- End Users must not construct passwords that are identical or substantially similar to passwords that they had previously used. IT Systems and Infrastructure should be configured so that End Users are not permitted to reuse at least the last 6 passwords.
- User accounts that have system-level privileges granted through memberships or programs such as SQL Administrator or AD Administrator must have a unique password from all other accounts held by that user.

7.3 Password Storage

The display and printing of passwords must be masked, suppressed, or otherwise obscured in such a way that unauthorized parties will not be able to observe or subsequently recover them.

- Passwords must always be encrypted when transmitted over networks;
- Passwords that need to be recorded on paper should be housed in a locked, secure environment. Passwords must not be written down and left in a place where unauthorized persons might discover for example: Never put your password on a sticky note on PC or your desk.

7.4 Password Changes

- All End Users should change their passwords at least once every thirty (30) days. This forced change should be automated wherever it is supported;
- Passwords will expire every 30 days. If the password is not reset within 10 working days of expiry, the relevant account will be disabled. End Users will need to use Help Desk to re-enable this account.
- When a password has been compromised, it should be changed immediately;
- All password resets require the End Users to identify themselves to the help desk staff using up-to-date unique information in the organization directory.
- Passwords shall not be disclosed to an end-user via e-mail, instant messaging, or any other form of electronic communication including verbally. It shall only be sent to the mobile number recorded on the Exchange Directory.
- In the event of a user who does not have access to a mobile telephone, the user should physically identify himself or herself to a supervisor in the Help Desk by means of their ID document, where after the Help Desk Agent will verbally supply the user with a password.
- A person may only request his or her own password be reset. End Users can register on the electronic password system to reset their own passwords on the Password Self-Service tool where applicable.
- Reset passwords may not be a word found in the dictionary or some other part of speech for example, proper names, places, and slang. Administrators must use a Random Password Generator to compile the use once password.
- The initial passwords issued by a System Administrator must be valid only for the concerned End User's first on-line session. The End User must be forced to choose another password before any other work can be done.

8 ROLES AND RESPONSIBILITIES

8.1 RLM employees, Contractors and Agents

RLM employees, contractors and agents are responsible for the following:

(a) Ensuring their passwords are not compromised in any way;

(b) Their personal details are always up to date on all electronic systems such as ERP and AD, this can be done via a request to the helpdesk; and

(c) Take reasonable care in choosing their passwords.

8.2 System Administrators

System Administrators are responsible for the following:

(a) Ensuring passwords are not compromised in any way;

(b) The Random Password Generator is used to reset password at all times; and

(c) No user is to receive any password by any means other than a SMS to the number recorded on the AD.

9. BREACH

Where a breach of this policy has occurred, appropriate disciplinary action will be taken in line with RLM's relevant policies.

EXEMPTION

The Chief Information Officer has the sole right to exempt a person or application from this policy, or part thereof. The exemption will be null and void unless:

(a) It is in writing;

(b) It is signed and dated by the Chief Information Officer;

(c) The Internal Audit Department is notified of the exemption; and

(d) A record is kept of the exemption.