BERGRIVIER MUNICIPALITY

PASSWORD POLICY

APRIL 2012

PASSWORD POLICY

REVISION NUMBER	DATE	AUTHORISEDFORDISTRIBUTION

1. INTRODUCTION

A computer access password is the primary key to computer security. The importance of password maintenance and security cannot be over emphasised. All employees and users of the Bergrivier Municipality's computer facilities are solely responsible for the integrity and secrecy surrounding passwords allocated for their usage. The password uniquely identifies employees and users, and allows access to the Bergrivier Municipality's information and computer services. For the users protection, and for the protection of Bergrivier Municipality's resources, the password must be kept secret and not be shared with anyone else.

The IT Department should be contacted if any further password information is required, or if there is any uncertainty surrounding the usage, applicability, and installation or issuing of passwords.

2. PASSWORD POLICY

All user-chosen passwords for computers and networks shall be difficult to guess. Do **not** choose:

- Words in a dictionary
- Proper nouns
- Geographical locations
- Common acronyms
- Slang
- Derivatives of user-IDs
- Common character sequences such as "123456"
- Spouse's name
- Children's/boyfriend's/girlfriend's/pet's names
- Car license plate
- Your ID number/birth date

Do **not**:

- Construct fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change.
- Construct passwords which are identical or substantially similar to passwords previously employed.
- Write down or otherwise record a readable password and store it near the access device to which it pertains.

Further policy statements:

- Passwords shall not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorised persons might discover or use them.

- All vendor-supplied default passwords shall be changed before any computer or system is used.

- All passwords shall be changed immediately if they are suspected of being disclosed, or known to have been disclosed to unauthorised parties.

- Regardless of the circumstances, passwords must never be shared or revealed to anyone else by the authorised user.

- Employees and users:

  - Are responsible for all activity performed with their personal user-IDs

  - Shall not allow the user-IDs to be used by anyone else

  - Shall not perform any activity with other users' IDs.

- Employee and user generated passwords should in general have the following characteristics:

  - Be at least 8 characters in length

  - Passwords should be made up of characters using : Alpha (alphabetical letters), numeric (whole numbers), upper & lower case and symbols.

  - Not contain the user-ID as part of the password

  - Be changed at least every 30 days for systems that do not automatically force regular password changes.

  - "Screen savers" should be activated after 10 minutes of inactivity as a maximum, and should be password controlled.

Certain systems have specific password requirements over and above those shown above. These systems will prompt the user for the correct information. If in any doubt, contact the IT Department for further information.

Should you forget your password contact the IT Department for assistance. Please be aware that the IT Department personnel are not permitted to automatically reset or reissue passwords. Replacement passwords will only be issued once certain prescribed security checks have taken place and this process may take some time to complete.

Refer to the IT Department for details on Password resets. Please note though that according to the agreed Security Procedures, passwords will only be issued if the person to whom the password is being issued is identifiable.