POLICY: **PASSWORD**

Item A-ICT (4-2004) CM 24/06/2004	INFORMATION AND COMMUNICATION TECHNOLOGY DEPARTMENT: POLICIES AND DISCLAIMERS

RESOLVED:

1. That the contents of the report regarding the Password, Internet and E-Mail Policies as well as the E-Mail and Network Login Disclaimers **BE NOTED**.

2. That the policies and disclaimers referred to in (1) above and attached as Annexure ”A” to “E” to the report **BE APPROVED** and **IMPLEMENTED** and **BE PUBLISHED** on the Intranet.

3. That the Executive Director: Information and Communication Technology **SOLICIT** comments from all departments on the policies referred to in (2) above and **SUBMIT** a report thereon by end of July 2004.

ANNEXURE A – PASSWORD POLICY

1 INTRODUCTION

The password policy is devised to assist in providing the required access security with regard to the systems and their relevant information within the Information and Communication Technology Department of Ekurhuleni Metropolitan Municipality. The policy is aimed to protect both the Information Technology business unit and its employees in respect of the control of access and right to information by determining the principles and rules, which govern the password security function.

2 POLICY STATEMENT

The specific purpose of the password policy is to establish controls and procedures to ensure that passwords are correctly administered and managed by the department.

3 SCOPE

The policy shall apply to all staff within the Information and Communication Technology Department of the Ekurhuleni Metropolitan Municipality. The policy will include the rules governing passwords.

4 RELATED POLICIES

None.

5 BUSINESS RULES

5.1.1 All user passwords will be set with a password age of thirty days.

5.1.2 Password expiry options will warn the user five days prior to the current passwords expiration.

5.1.3 Login time intervals will be set to three hundred seconds.

5.1.4 All user passwords will be set with a minimum password length of eight characters.

5.1.5 Password uniqueness will be set to cater for twelve new passwords before a password can be reused.

5.1.6 Password lockout will be set at five failed logon attempts.

5 1 7 To have a password reset the user will contact the helpdesk The helpdesk will request confirmation to reset the password from the users supervisor Only then will the password be reset for the user

5 1 8 Blocked accounts will only be reset by the system administrator

5 1 9 Passwords of key role holders - such as System and Network administrators – will be copied and held under dual control in a fire-resistant, secure location, to enable access to the system by an authorised person in the unavoidable absence of the password holder

6 NON COMPLIANCE WITH THE POLICY

Ekurhuleni will take any disciplinary action arising from breach of this policy according to the disciplinary code and grievance procedure of the Ekurhuleni Metropolitan Municipality

7 MAINTENANCE OF POLICY

Maintenance is the responsibility of the Information and Communication Technology Department of the Ekurhuleni Metropolitan Municipality