**5.1. Access Control Policy**

1. Access to information shall be controlled based on business and security requirements and the access control rules defined for the system. These rules shall include the followings:

a. Both logical and physical access controls.

b. Security requirements of organizations

c. An identified business requirement for the user to have access to the information or business process (both ‘need-to-know’ and ‘need-to-use’ principles).

d. All access is denied unless specifically approved under the provisions of this policy

e. Changes in user permission whether performed automatically or by an administrator.

f. Legal and/or contractual obligation to restrict and protect access to systems.

2. Access for contractors or third parties personnel to organiation assets shall be provided only based on a contractual agreement. This agreement shall include, but not be limited to:

a. The terms and conditions for access provided.

b. The security responsibilities of the contractors or third parties personnel.

c. Agreement by the contractors or third parties personnel to organization’s information security policies