

**Organization Manual  
Section 2 - Policies**

**CEMIG Companhia Energética de Minas Gerais**

**NO-02.05 Alt. 01**

**06/28/2005 Pg.01**

**INFORMATION SECURITY POLICY**

**Replaces NO -02.05 of 09/05/96**

**1. INTRODUCTION**

Information security is the responsibility of everyone at Companhia Energética de Minas Gerais – CEMIG and its value chain. Shareholders, executives, employees, clients, suppliers and partners must take care to safeguard their activities and concerns with adequate information and system protection means, as information is an important competitive differential.

Information security actions can reduce costs and increase revenues for the Company, via processes, products and services supported by secure information systems. In addition, business risks can be further reduced and better managed, strengthening the Company's image and adding value to Cemig and its shareholders.

**2. CONCEPT**

2.1 **Confidentiality:** guarantees information security in the sense that access is granted solely to authorized personnel.

2.2 **Availability:** guarantees that authorized users have access to information and related data whenever necessary.

2.3 **Integrity:** safeguards the accuracy and comprehensiveness of the information and processing methods.

2.4 **Legality:** guarantees that the information conforms to the legislation in force.

2.5 **User:** employees, interns, contract employees, service providers, partners and suppliers that utilize the Company information.

**3. BASIC PRINCIPLES**

3.1 CEMIG adopts clear and well defined criteria for its Information Security Policy, guaranteeing its alignment with the Company's strategic directives and legal and regulatory requirements.

3.2 The organ responsible for the information security process and the other Company organs are aware of this policy and aligned with the same for the same objective, cooperating together to achieve the desired results.

**4. DIRECTIVES**

#### 4.1 Information is an asset

Information is a valuable and legally protected asset, which constitutes a competitive differential. Information generated, acquired, processed, stored, transmitted and discarded is considered to be CEMIG property and should be adequately protected. The release of strategic Company information must have previous authorization.

**J:\USERS\RH\RHDO\M ORGANIZACAO\02 Politicas\PoliticaSegurançadalInformação.doc**

### **Organization Manual Section 2 - Policies**

#### **CEMIG Companhia Energética de Minas Gerais**

#### **NO-02.05 Alt. 01**

#### **06/28/2005 Pg.02**

#### 4.2 Information Protection

Information protection measures should take the following into consideration:

- adequate levels of integrity, confidentiality and availability;
- legislation, judicial decisions, directives and general and restrictive instructions and procedures in force;
- the Declaration of Ethical Principles and Code of Professional Conduct;
- the cost / benefit ratio;
- alignment with CEMIG's strategic directives;
- the best Information Security Management practices;
- the appropriate behavioral and technological aspects.

#### 4.3 Information Security Responsibility

Each user is responsible for Information Security at CEMIG and should know, understand and obey the directives, Declaration of Ethical Principles and Code of Professional Conduct and the general Procedural Instructions and any restrictions applicable to their activities, striving to correctly apply all protection measures.

#### 4.4 Access to Information

4.4.1 The access and use of any Company information should be limited to that which is necessary to the performance of the user's professional activities within the scope of CEMIG.

4.4.2 When accessing electronic systems, only systems and technologies authorized by CEMIG should be employed, via personal and non-transferable key accounts and passwords.

### 5. GENERAL GUIDELINES

5.1 All procedures related to Information Security that are defined in specific instructions must be in accordance with this Policy. Once released, they become an integral part of this Policy.

5.2 Failure to observe the Information Security Policy will be considered an act of disobedience, subject to the application of internal administrative sanctions and any sanctions stipulated in the legislation in force.

**DJALMA BASTOS DE MORAIS**

**CEO President**

Distribution: General

**J:\USERS\RH\RHDO\M ORGANIZACAO\02 Politicas\PoliticaSegurançadalInformação.doc**