Information Security Policy
for
Protection of Critical Information Infrastructure

Doc No.: CERT-In/NISAP/01, Issue 01, May 2006

Indian Computer Emergency Response Team (CERT-In)
Department of Information Technology, Govt. of India,
Electronics Niketan, 6 CGO Complex, Lodhi Road, New Delhi – 110003

1.0 Background

1.1 Security relates to the protection of valuable assets against loss, misuse, disclosure or damage. In this context, “valuable assets” are the information recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium. The information must be protected against harm from threats leading to different types of vulnerabilities such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional damage. Protection arises from a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics and firewalls. These safeguards should address both threats and vulnerabilities in a balanced manner.

1.2 In the ever-changing technological environment, security must keep pace with these changes to enable organisations to create and operate in an environment of **‘Trust and Confidence’**. It must be considered an integral part of the systems development life cycle process and explicitly addressed during each phase of the process. Security must be dealt with in a proactive and timely manner to be effective.

1.3 For most organisations, the security objective is met when:

- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from failures *(availabilit*y)
- Information is observed by or disclosed to only those who have a right to know *(confidentialit*y)
- Information is protected against unauthorised modification *(integrit*y)
- Business transactions as well as information exchanges between organisation locations or with partners/users can be trusted *(authenticity* and *non-repudiatio*n)

2.0 Introduction

2.1 With the increasing use of information technology, functions in Government and businesses are now increasingly dependent on network of critical information infrastructure. As such, any disruption of the operation of information systems of critical infrastructure is likely to have a devastating effect on people, economy, essential human & Government services and National security.

2.3 In view of the potential impact, protection of critical information infrastructure is essential to ensure that disruptions are infrequent, of minimal duration & manageable and cause the least damage possible.

2.4 Users of information resources must have skills, knowledge, and training to manage information resources, enabling the organisations to effectively serve the customers/users through automated means.

2.5 Personnel with program delivery responsibilities should recognize the importance of security of information resources and their management to mission performance.

3.0 Purpose

Recognizing the growing networked nature of the computing environment in Government as well as critical sector organisations and the need to have proper methodological vulnerability analysis and effective management of information security risks, Department of Information Technology (DIT) has been mandated to put in place an Information security policy for protection of critical information infrastructure in the country and ensure compliance.

4.0 Information security policy

In order to reduce the risk of cyber attacks and improve upon the security posture of critical information infrastructure, Government and critical sector organizations are required to do the following on priority:

- Identify a member of senior management, as Chief Information Security Officer (CISO), knowledgeable in the nature of information security & related issues and designate him/her as a ‘Point of contact’, responsible for coordinating security policy compliance efforts and to regularly interact with the Indian Computer Emergency Response Team (CERT-In), Department of Information Technology (DIT), which is the nodal agency for coordinating all actions pertaining to cyber security
- Prepare information security plan and implement the security control measures as per IS/ISO/IEC 27001: 2005 and other guidelines/standards, as appropriate
- Carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organisational goals/objectives.
- Periodically test and evaluate the adequacy and effectiveness of technical security control measures implemented for IT systems and networks. Especially, Test and evaluation may become necessary after each significant change to the IT applications/systems/networks and can include, as appropriate the following:

  – Penetration Testing (both announced as well as unannounced)
  – Vulnerability Assessment
  – Application Security Testing
  – Web Security Testing

- Carry out Audit of Information infrastructure on an annual basis and when there is major upgradation/change in the Information Technology Infrastructure, by an independent IT Security Auditing organization

  Note: Government and critical infrastructure organizations can make use of CERT-In evaluated and empanelled third party agencies for their organisation / site specific Information security assessment services (including ISMS assessment, risk assessment, network security profiling, penetration testing, vulnerability assessment, application security testing etc) under specific contract and pre-determined rules of engagement. Contact details of the agencies empanelled by CERT-In are available at ‘http://www.cert-in.org.in’

- Report to CERT-In the cyber security incidents, as and when they occur and the status of cyber security, periodically.