Policy Name: Information Management

Policy Number: I/T100
Policy Owner: Vice President and Chief Information Officer
Policy Approver: President and Chief Executive Officer
Approval Date: May 1, 2011

Policy Statement:

This Information Management Policy is about people, technology and information. It supports Nexen by ensuring that the use and management of information and technology are aligned with the corporate culture of integrity and professional conduct. It is not intended to impose restrictions that are contrary to Nexen's established culture of openness and trust but rather for protecting the company, its Employees and Contractors and its partners from illegal or damaging actions resulting from the improper use of our Information Assets, our Information Technology (I/T) Assets, and our I/T Services. Nexen is committed to the protection and management of information and its supporting technology in alignment with defined requirements for business operational, contractual, legal and regulatory obligation.

1. Definitions:

Company (or Nexen) – Refers to Nexen Inc. and its majority owned subsidiaries.

Contractor – Means any person or entity, including their employees or sub-contractors that have been contracted, sub-contracted, or otherwise engaged to provide services to the Company. The Contractor may be identified by, but not limited to, such terms as third party, direct hire, independent or contractor.

Employee – Means a regular full-time, part-time, temporary, casual or fixed-term employee of the Company.

Information Asset – Refers to all information regardless of format, including electronic and paper based, and the systems and infrastructure used for the capturing, transporting, alteration and storage of company information.

I/T Asset – Information technology, including networks, computers, applications and software or Information, including documents, files and data that are owned or controlled by Nexen.

I/T Services – Information technology services, including e-Mail, access to the Internet, wireless access or any other form of electronic enterprise service provided by Nexen.

Policy - Refers to a course of action or principle of conduct adopted by the Company which directs organizational actions and Employee conduct. It expresses an attitude, intent or Company position which serves as a broad directive in the conduct of the Company's business and its relationships with its Employees.

2. Objectives:

The objective of this Policy is to ensure that Employees and Contractors have a clear understanding of the corporate expectations relative to the creation, use and management of information and technology within the Company.

3. Persons Affected:

This policy applies to all Employees, Contractors or other individuals who use or access Nexen I/T Assets or I/T Services.

4. Policy:

Nexen recognizes that information and its supporting information technology is critical to any successful business operation. Information, in any format, is a valuable corporate asset and should be properly protected and managed throughout its lifecycle. Nexen's corporate information will be managed in alignment with internal and external contractual, legal and regulatory requirements.

This policy and its associated code of practice support those objectives from three perspectives:

- Nexen provides Information Technology (I/T) Assets and Services to Employees and Contractors to meet the requirements of the business. They are designed and managed to balance efficiency with cost, and to protect Nexen from illegal or damaging actions, either knowingly or unknowingly, resulting from improper use or actions.

- Policy with respect to acceptable and unacceptable use is in place to protect both the personnel and Nexen. Inappropriate use could expose Nexen to risks including diminished reputation, loss of intellectual property, compromise or network breach and the disruption of network systems and services.

- All business Information Assets, regardless of format or content, should be classified and properly managed. Once classified, the information shall be subject to appropriate levels of control to protect it from accidental or unintentional loss, unauthorized manipulation or improper disclosure either within Nexen or externally.

Nexen employees are required to:

- Read and understand this policy and its associated code of practice. If any area is not clear, they should seek out clarification from management.

- Work within the confines of implemented I/T controls installed to protect Nexen from harm.

- Assume personal responsibility for the protection of Nexen's Information Assets, where possible, and to report infractions or incidents.

- Protect Nexen Information Assets and Services in accordance with this policy.

5. Roles and Responsibilities:

- **Employees and Contractors at Nexen**

  All persons, either Employees or Contractors, using Nexen Information Assets are required to understand and comply with this policy.

- **Supervisors/Managers**

  Supervisors and Managers are responsible to ensure that all of the Employees and Contractors at Nexen in their charge are aware of this policy. Requests for exemptions to this policy or special consideration should be directed by the manager, for their reports to the Manager of I/T Security.

- **Manager of I/T Security**

  The Manager of I/T Security is responsible for the management and updates of this policy.

- **Vice President, Chief Information Officer**

  The Vice President, Chief Information Officer is the owner of this policy and is responsible for its implementation within the company.

- **President and Chief Executive Officer**

  The President and Chief Executive Officer is responsible for approval of this policy. The President and Chief Executive Officer is also responsible for setting the vision of the company in conjunction with the Executive Management Committee and the Board of Directors.

6. Compliance:

- **Employee Monitoring**

  Nexen owns all corporate I/T Assets and Services and as such retains the right to monitor and audit all corporate resources and the activities related to their use.

- **Disciplinary Action**

  Employee and Contractor acceptance and continued efforts to comply with the guidance and rules described in this document will contribute to the availability, performance and security of Nexen's corporate information and technology. Failure to comply with this policy may result in disciplinary action up to and including termination of employment or the termination of a contract.

7. Guiding Principles / Related Policies:

The following Company policies and guides may also be consulted:

- I/T Acceptable Use Policy (I/T 200)
- Information Classification and Protection Policy (I/T 201)
- I/T Governance Policy (I/T 202)
- How We Work – Our Integrity Guide (A099)
- Privacy of Personal Information Policy (A 106)
- Human Resources Strategy (HR 100)

8. Revision History:

DATE	REVISION #	DESCRIPTION OF CHANGE
May 1, 2011	Policy Creation	This Tier One Policy was created to align with new policy re-formatting standards. It incorporates and aligns the contents of I/T200, I/T201 and I/T202 Tier two I/T policies and their associated codes of practice.