Information Security Policy

NTT DOCOMO GLOBAL, INC (hereinafter referred to as "NDG") recognizes that proper information management is an important management issue, therefore declares the Information Security Policy as NDG's action policy for information security and will abide by the Information Security Policy in order to ensure that customers are able to deal with NDG safely.
Information assets to which the Information Security Policy applies shall mean information obtained or learned in the course of NDG's business activities, as well as all information owned by NDG for business purposes.

1. Establishing Information Security Management System
   NDG establishes a system that can quickly implement information security measures by setting up an Information Management Committee and appointing an information management supervisor for each organization in order to protect all information assets owned by NDG and manage them properly.

2. Appointing Chief Information Security Officer
   NDG appoints the Chairman of the Information Management Committee as Chief Information Security Officer (CISO) in order to protect the information assets and manage them properly.

3. Developing Internal Rules
   NDG develops internal rules on information security and ensures that all employees abide by the clear policy and rules for protecting the information assets and managing them properly.

4. Developing and Operating Audit System
   NDG complies with various laws and regulations related to security, codes of conduct related to security formulated by administrative bodies and industry groups, internal regulations and rules, etc. when performing its operations. NDG performs information security audits regularly and as necessary in order to verify that these security frameworks are functioning effectively and responds strictly if there have been any violations in order to ensure appropriate information management.

5. Proper Information Security Measures
   NDG carries out security measures from the perspective of organizational, physical, technical, and human security management in order to prevent accidents from happening to the information assets, such as unauthorized access, data corruption, information leakage, or tampering. These measures are continually improved though modifications as necessary when there are technical or social needs in order to adapt to those changes.

6．Improving Information Security Literacy
　　NDG continuously provides education and training to all employees in order to
　　ensure that information security literacy is improved and the information
　　assets of NDG are managed properly.

7．Strengthening Subcontractor Management System
　　NDG fully examines the appropriateness of subcontractors before signing a
　　contract and requires them to maintain the same or higher level of security as
　　NDG. Furthermore, NDG regularly performs audits for its subcontractors in order
　　to ensure that their security level is maintained properly.

8．Performing Continuous Improvement
　　NDG performs continuous improvement of information security management by
　　regularly evaluating and reviewing the above activities.