Information Security Policy

1. Purpose

Based on the “Guiding Principles at Toyota” and “Toyota Code of Conduct”, Toyota Motor Corporation (hereinafter called, “TMC”) and TMC’s consolidated subsidiaries (hereinafter collectively called, “Toyota”) understands that Information; such as trade secrets and personal information; created by Toyota or received from customers, business partners or other entities in the course of business activities, associated information management systems and the control systems of Toyota’s products and facilities (hereinafter called, “Information Assets”) are critical assets for Toyota’s business activities.

Based on the above understanding, TMC establishes Information Security Policy (hereinafter called, “The Policy”) to ensure that Toyota manages and practices information security methodically and continuously.

2. Toyota’s basic approach to information security

1) Compliance

Toyota shall comply with applicable laws, governmental guidance, contractual obligations and other social norms related to information security.

2) Maintenance of stable business infrastructure

Toyota shall ensure competitiveness and business continuity through the management and protection of its Information Assets.

3) Providing safe products and services

Toyota shall incorporate information security practices into Toyota’s business activities such as the development, design and production processes of products and services in order to provide safe products and services to customers.

4) Contribution to the establishment of safe Cyberspace

Toyota shall act as a good corporate citizen by contributing to a safe online environment (“Cyberspace”) by working to identify and mitigate information security vulnerabilities in Toyota’s Information Assets.

5) Information Security Management

Toyota shall continuously implement information security management through the establishment of governance and risk management including incident response.