Safe Environment for Information and Communication Security

In order to secure information and communication operations, the Administration has gradually been building an information security defense system such as firewall system to control the connection and service between computers inside and outside of the Park. Anti-virus software was installed in both mainframes and end users to instantly detect and remove infected files as well as blocking e-mail .exe files and macro files in order to reduce the risk of computers being infected. An Intrusion Detection System was also installed to detect any possible attacks to information equipment and Internet systems by hackers. The Administration carried out vulnerability scanning irregularly so as to locate any loopholes, and hence, minimize the opportunities for hackers to intrude.

In addition, the Administration built a "Disaster Recovery Plan and Procedures for Information System" to prevent information equipment from any failures, which might cause information service breakdown. Important files were backed up everyday, and they were stored off-site to ensure information security. The "Disaster Recovery Test" was drilled more than once (included) each year, and the test result was used as a reference for future improvement, so that the feasibility and applicability of the "Disaster Recovery Plan and Procedures for Information System" could be established.