## Policy on Information Technology Governance

In line with the rapid development of banking technology, the Company needs to have a Guide to Information Technology Governance. The Company's Guide to Information Technology Governance consists of several policies including, among others, the guidelines on information technology risks, information technology change management, information technology problem management, information technology quality control, information technology capacity management, information technology communication network management and data center physical security. Such guidelines include, among others, the policy and procedure for handling and mitigating risks. The Company has also measured the information technology maturity level. The Company has implemented information technology governance policies effectively.

Below are several things related to the management of Information Technology Governance in the Company:

### Cyber Security and Disruption

The Company operates a number of policies on cyber security and disruption to prevent cyber-attacks and to secure the Company itself.

List of Policies

| No. | List of Policies |
|---|---|
| 1 | Basic Policy on IT Risk Management |
| 2 | Information Security Policy for Regional Offices and Branches |
| 3 | Information Security Policy for Head Office |
| 4 | Information Security Manual for Regional Offices and Branches |
| 5 | User ID and Password Management Manual |
| 6 | RACF Security Guide |
| 7 | Key Management System Security Guide |
| 8 | Network Security Guide for Head Office |
| 9 | Network Security Guide for Regional Offices/Branches |
| 10 | Tandem Security Guide |
| 11 | UNIX (Solaris) Security Guide |
| 12 | Linux Security Guide |
| 13 | User ID and Password Security Guide |
| 14 | Windows Security Guide |
| 15 | Operations Manual for LAN Security Management |

| | |
|---|---|
| 16 | Base24 Security Manual |
| 17 | BDS IBS Security Manual |
| 18 | CardLink Security Manual |
| 19 | Host to Host ERP Key Management Manual |
| 20 | Operations Manual for Tandem Security System |
| 21 | Wireless Local Area Network (WLAN) Installation Guide |
| 22 | Guide to Using Social Media, Internet and Emails |
| 23 | Guide to Safeguarding ATMs |
| 24 | BYOD Security Guide |
| 25 | Remote Access |

Implementation

Implementation of governance related to Cyber Security in the Company:

- Building awareness among all Branch offices/Regional Offices by paying visits to the Branches/Regional Offices to hold Discussion Forums or Regional Coordination Meetings.
- Building awareness among all Head Office staff in the form of COP (Community of Practice)
- Requiring all staff at the Head Office/Branches/Regional Offices to participate in e-learning
- Making cyber security videos to build awareness and playing them on the Head Office's media (TV media)
- Sending emails for awareness to all staff at the Head Office/Branches/Regional Offices
- Conducting a phishing test to all staff having the right to access bca.co.id
- Conducting a discussion on Information Technology during 2018 at the BOD's or BOC 's meeting.

Assessment

Based on the assessment carried out by the Ministry of Communication and Information Technology in 2018, the Company has implemented excellent Cyber Security.

### Disaster Recovery

The Disaster Recovery and Emergency Management Policy is regulated by the Integrated Business Continuity Policy for the Company's Financial Conglomerates, as evident from Decision Letter of the Board of Directors No. 180/SK/DIR/2017 dated 11 December 2017. The Integrated Business Continuity for the Company's Financial Conglomerates constitutes the implementation of Business Continuity to ensure the business continuity of the Company and the Members of the Company's Financial Conglomerates when certain disruption occurs. Such policy includes the business continuity plan policy, the protocol from the Company to the members of the Company's Financial Conglomerates and vice versa as well as the Recovery priority order.

| | |
|---|---|
| Background | The Company's operational activities are prone to disruption/damage that may be caused by nature or humans. The damage may have adverse effect not only on the Company's technological capabilities but also on the Company's business operations, especially services to the customers. |
| As regards the BCM | To minimize the risks mentioned above, the Company implements Business Continuity Management (BCM). BCM is an integrated and comprehensive management process regarding the potential impact that may arise if the Company's critical business function fails due to disruption/disaster, intended to protect the interests of stakeholders. BCM is an integral part of the Company's Risk Management Policy as a whole. |
| Support | In order for the BCM to operate effectively, the Company's BCM is supported by:<br>• active involvement of the management.<br>• implementation of Risk Assessment and Business Impact Analysis.<br>• preparation of proper Business Continuity Plan (BCP).<br>• implementation of BCP testing.<br>• Monitoring by the Internal Audit Division. |