204 DEMAND DEPOSITS OF BANK OFFICERS AND EMPLOYEES

As a general rule, officers and employees of banks, their spouses and relatives within the second degree of consanguinity and affinity, including partnerships, associations or corporations in which such officers and employees, their spouses and relatives within the second degree of consanguinity and affinity, individually or as a group, own or control at least a majority of the capital are prohibited from maintaining demand deposits or current accounts with the banking office in which they are assigned. However, officers and employees without direct access and involvement in the handling of transactions and/or records pertaining to demand deposit operations may be allowed to maintain demand deposits or current accounts in the banking office where they are assigned subject to the following conditions:

a. It shall be the responsibility of the bank concerned to identify the officers, employees, departments or units with direct involvement in its demand deposit operations and/or deposit records;
b. The opening of current accounts of officers and employees shall be subject to approval of the head of the branches department or any designated higher ranking officer; and
c. The following minimum operating control measures shall be implemented to ensure systems integrity and mitigate technology-related risks:

(1) *Tagging of accounts.* Savings and demand deposits of officers and employees, their spouses and relatives within the second degree of consanguinity and affinity, including partnerships, associations or corporations in which such officers and employees, their spouses and relatives within the second degree of consanguinity and affinity, individually or as a group, own or control at least a majority of the capital shall be tagged in the bank's current accounts/savings accounts (CA/SA) system;

(2) *Monitoring of accounts.* All accounts maintained by officers, employees and said relatives including their business interests shall be monitored by a designated officer who shall be responsible for ensuring that accounts of officers and staff are properly maintained. Any irregularity in the account activity shall be promptly investigated and reported to the appropriate management level;

(3) *Access controls.* Access to all data, application software, operating systems and utilities must be restricted to authorized persons through appropriate identification mechanisms and access codes and such authentication and authorization controls must be fully documented and auditable. No officer or employee, regardless of rank or position, shall be allowed to process any transaction from initiation to final authorization;

(4) *Data capture.* Operating procedures for data capture, update and retrieval must be strictly

adhered to. The operating system shall maintain a permanent record of each authenticated user session including every user input; and

(5) *Audit trails.* Detailed records and audit trails shall be maintained to substantiate the processing of all transactions. Audit trails must be reviewed periodically by a designated officer commensurate with the risk level of the information system. The review process must ensure that the reviewer does not review his/her own activity.