Policy 1329: Segregation of Duties Conflict Resolution

Policy No.: 1329

Responsible Officer: Senior Vice President, Finance and CFO

1.0 Purpose

To establish the Company's position on the elimination and/or mitigation of segregation of duties ("SOD") conflicts within the Company's Enterprise Resource Planning ("ERP") system(s).

2.0 Definitions

2.1 Segregation of Duties: An internal control concept that a single individual does not have the ability to perform incompatible and critical functions within the information technology environment. Key processes should have a shared responsibility within the Company to mitigate the risk of noncompliance and fraudulent activity.

2.2 Enterprise Resource Planning System(s): PRDCLNT400 and SEPCLNT400.

2.3 Governance, Risk, and Compliance ("GRC") Access Control: A software tool utilized by the Company to automate the process of managing an ERP individual's system access and to monitor SOD risk violations.

2.4 Internal Control: A process, effected by the Company's Leadership Council, senior management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

2.5 Preventive Control: A control designed to prevent the occurrence of an undesirable event.

2.6 Detective Control: A control designed to detect the occurrence of an undesirable event.

2.7 Personal Identifiable Information ("PII"): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

2.8 Security Profile: A set of rights and restrictions that can be associated with an individual or group of individuals. The security profile determines the actions, such as viewing, creating, and editing, that an individual can perform on various resources, such as master data.

2.9 Risk Owner: An individual assigned to SOD risks, who is commonly responsible for approving changes to SOD risk definitions and violations of the SOD risk. The individual may also receive conflicting and critical action alerts.

2.10 Role Owner: An individual responsible for approving either role content or individual role assignment or both.

2.11 Mitigation Monitor: An individual assigned to mitigation controls to monitor activity and who may receive mitigation control monitor alerts.

2.12 Mitigation Approver: An individual assigned to mitigations controls and who is responsible for approving changes to the mitigation control definition and assignments.

3.0 Policy

3.1 SOD Conflicts Risk Profile

The Company must eliminate and/or mitigate critical, high, and medium risk SOD conflicts created as a result of access assigned to an individual within the Company's ERP system(s), in accordance with the Policy.

The Company's Staff/Business Units must eliminate or mitigate SOD conflicts within the ERP System(s), in order to safeguard assets, manage access to confidential information (i.e. intellectual property, trade

secrets) or sensitive information (i.e. PII), and improve the quality of internal controls over business critical information.

3.2 Elimination or Mitigation of SOD Conflicts

3.2.1 A manager's or supervisor's job responsibilities must include procedural controls designed to prevent and detect fraud or inadvertent errors during the course of normal business operations. Data integrity is critical in the processing of business transactions. Accordingly, the following procedures must be followed in assigning or changing an individual's ERP system security access and authorization profile.

3.2.2 If an individual needs access to transactions within the Company's ERP system(s) to perform a certain job function or responsibility, the individual must submit a BetterNet request to assign the transactions to the individual's respective ERP system security profile.

3.2.3 The Information Technology Security Department will obtain a documented approval confirmation from the individual's manager or supervisor before assigning the transactions to the individual's ERP system security profile.

3.2.4 If approved, the Information Technology Security Department will perform an SOD assessment in the GRC Access Control software tool. The SOD assessment will identify the SOD conflicts within the individual's ERP system security profile, if any, as a result of assigning the transaction(s). If an SOD conflict is identified in the SOD assessment, the following procedures will be followed to eliminate or mitigate the SOD conflict:

a. The SOD assessment will be sent to the Senior Director, Internal Audit, to evaluate the SOD conflicts. The Senior Director, Internal Audit, will ask for an explanation from the individual's manager or supervisor on the ERP system access request and question if the request is (1) a permanent ERP system access request to perform certain a job function or responsibility or (2) a temporary ERP system access request to perform certain a job function or responsibility as a back-up to a primary.

b. If the Senior Director, Internal Audit, deems the request to be appropriate and a pre-approved mitigation control is in place, an approval will be provided to the Information Technology Security Department to assign the approved mitigation control maintained within the GRC Access Control software tool and assign the requested access to the individual's ERP system security profile.

c. If the Senior Director, Internal Audit, deems the request to be appropriate and a pre-approved mitigation control is not in place, they will have a conversation with the individual's manager or supervisor and Internal Audit Department on developing a mitigation control to mitigate the SOD conflict. The Information Technology Security Department will not be granted the authorization to assign the access to the individual's ERP system security profile without the pre-approved mitigation control. If an emergency situation is present that requires immediate action due to a business critical function, the Senior Director, Internal Audit, has the designated authority to provide an approval to the Information Technology Security Department to assign the requested access to the individual's ERP system security profile on a temporary basis without a pre-approved mitigation control in place.

d. The organizational structure in the GRC Access Control software tool has a designated a risk mitigation monitor and a risk mitigation approver for each mitigation control.

4.0 Responsibilities

4.1 Individuals with direct and indirect reports are responsible for:

a. Awareness and understanding of the SOD conflicts and pre-approved mitigation controls for direct or indirect reports.

b. Alignment with the Information Technology Security Department and the Senior Director, Internal Audit, when individuals transfer in and out of a Staff/Business Unit. The individual's ERP system security profile must be reviewed and adjusted accordingly, even if the individual is performing duplicate job roles during a defined transition period.

4.2 The Information Technology Security Department is responsible for:

a. Maintaining the GRC Access Control software tool.

b. Executing an SOD assessment for requests to change an individual's ERP system security profile or create a new individual's ERP system security profile. The report will be provided to the Senior Director, Internal Audit for review and approval.

c. Ensuring that the SOD conflicts are approved by the Senior Director, Internal Audit, before assigning an individual access in the ERP system.

d. Distributing SOD mitigation reports, as requested, from the GRC Access Control software tool.

4.3 The Senior Director, Internal Audit, is responsible for:

a. Ensuring that the critical, high, and medium risk SOD conflicts have pre-approved mitigation controls in place.

b. Reviewing the SOD mitigation reports to assess each individual's SOD conflicts and the ongoing need based upon the individual's job role and responsibility.

4.4 The Chief Financial Officer is responsible for the development and maintenance of these guidelines. The Leadership Council members and their direct reports are responsible for the enforcement of this Policy within their respective organizations.