CATALYST
WORKPLACES THAT WORK FOR WOMEN

SEGREGATION OF DUTIES STANDARD

Effective: September 1, 2020

Purpose of Standard

The purpose of this Standard is to define the activities which should be separated in order to achieve the objective of properly segregating conflicting duties. Segregation of duties has two primary objectives. The first is the prevention of conflict of interest (real or apparent), wrongful acts, fraud, abuse and errors. The second is the detection of control failures that include security breaches, information theft and circumvention of security controls. Organizational roles should be structured such that no one Resource (as defined below) is in a position to initiate, approve, and review the same action, transaction, event or process.

Application of Standard

This Standard applies to all Catalyst employees, contractors, vendors and agents (each, a ”Resource”) performing duties that require internal controls.

Standard

1. **Roles:** Management must identify and list relevant roles for the systems they oversee. Once identified, the Resources of the organization must be structured such that critical/operational functions are separated into distinct jobs. Examples of functions that should be segregated are:

    a. Entering financial transactions and approving them.

    b. Altering or destroying critical data and controlling detection mechanisms.

    c. Designing or implementing security controls and conducting security audits or reporting on the effectiveness of the controls.

    d. Exfiltrating sensitive information.

2. **Emergencies:** In certain emergency situations, which should be both temporary and infrequent in nature, segregation of duties may not be feasible. In these situations, Resources shall request elevated privileges, which must be approved by appropriate levels of senior management and fully documented as elevations of this nature represent a significant risk for loss.

3. **Compensating Controls:** Where segregation of duties cannot be consistently maintained by the organization or a department, management must rate the risk of non-adherence and mitigate the risk with compensating controls. At no time may the individual creating or approving the

compensating control have access to delete or modify audit trails. Examples of compensating control mechanisms that may mitigate a lack of segregation of duties are:

a. Audit trails enabling the re-creation of the actual transaction flow from the point of origination to its existence on an updated file. Audit trails must include the initiator of the transaction, date and time of entry, type of entry, data fields, and files updated.

b. Exception reports monitored at a supervisory level, supported by evidence that exceptions are reviewed, and if necessary, corrected in a timely manner. The review must be evidenced by signature of the supervisor and dated.

Violations of Standard

- **Non-Compliance.** An employee who violates this Standard may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

- None

Definitions and Terms

- None

Administration of this Standard

- **Questions.** You are encouraged to ask any questions you may have about this Standard. To learn more, please contact secure@catalyst.org.

- **Reporting.** It is important that you immediately report any suspected violation of this Standard by a Catalyst employee or third party to your manager or to HR. All good faith allegations of violations of this Standard will be fully and confidentially investigated.

- **Exception to Standard.** Limited exceptions to the Standard may apply due to variations in devices and platforms. Management does not have the authority to approve exceptions to this Standard. Any request for an exception to the requirements of this Standard must be submitted to the Information Security Officer, who will review the risk of non-adherence and issue exceptions where deemed prudent.

- **Applicability.** This Standard applies globally unless contrary to local laws and regulations. Operations in different countries may have more stringent policies or implementing procedures where required by local law. In the event of a conflict, these more stringent policies or implementing procedures will take precedence.

Revision History

Date	Name	Description	Responsibility
09/01/2020	James Mbassa	Initial release.	Owner