Attachment A

Segregation of Duties Policy, Procedures and Guidelines

1.0 Purpose

This document provides policy to ensure that system controls are implemented Job Corps-wide, as defined in the Policy and Requirements Handbook (PRH) Chapter 5. Segregation of duties is a primary internal control intended to prevent, or decrease the risk of errors or irregularities, identify problems, and ensure that corrective action is taken. This is done by assuring that no single individual should have control over all phases of a transaction.

2.0 Scope

This policy applies to all systems and applications that are operated on the Job Corps Network.

3.0 Policy

Job Corps Management and Points of Contact (POCs) are responsible for ensuring that access to all Job Corps information resources is documented and approved, as stated in PRH Chapter 5. Access to Job Corps Information Technology (IT) resources should be documented and approved based on the segregation of duties established for each Job Corps site. Job Corps access to IT resources should be established based on segregation of duties and least privilege. The following procedures and guidelines should be followed when establishing access based on duties.

The U.S. Department of Labor (DOL), National Office of Job Corps Policy and Requirements Handbook (PRH) states that Job Corps center operators and Outreach and Admissions/Career Transition Services (OA/CTS) contractors shall "submit written descriptions of control procedures to the contracting officer as part of the standard operating procedures in accordance with the schedule shown in Exhibit 5-1 (Standard Operating Procedures)." It also states "Control procedures shall include: 1) Separation of duties; 2) Approval requirements; 3) Documentation requirements." (PRH Chapter 5.7, R4)

3.1 General Guidelines

The following general guidelines should be used to determine the appropriate segregation of duties.

- Work responsibilities should be segregated so that one individual does not control all critical stages of a process. For example, a payroll clerk who enters student pay information must not authorize/approve pay.

- Segregation of duties should be achieved by dividing responsibilities between two or more individuals or organizational groups. Dividing duties among two or more individuals or groups reduces the likelihood that errors and wrongful acts will go undetected because of activities of one group or individual.

- Inadequate segregation of duties increases the risk that wrong or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources or data could be damaged or destroyed.

- The extent to which duties are segregated depends on the size of the organization and the risk associated with its facilities and activities. If centers are unable to implement the standard segregation of duties, more extensive supervisory oversight will be required to monitor/control activities. **Exhibit B** contains a list of duties that must remain segregated for both large and small organizations.

- Activities that involve large dollar transactions, or are otherwise inherently risky, should be divided among several individuals and be subject to extensive supervisory review.

- Segregation of duties must be divided among major operating and programming activities, including duties performed by users, application programmers, and the Job Corps Data Center (JCDC) staff.

3.2 General Roles and Responsibilities

Management

Segregate duties and establish related policies by:

- analyzing operations;

- identifying duties;

- assigning these duties to different organizational units or individuals; and,

- documenting functions and individual tasks performed by each group as part of the agency Standard Operating Procedures (SOP). A sample description of IT Technical Job Functions is in **Exhibit C**.

Note: Federal standards specify that key duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be segregated. This standard should also be applied to the authorization, testing and review of IT system changes.

User

Applications users are responsible for ensuring that they follow standard operating procedures as defined by management. For example, a payroll clerk who enters student pay information must not authorize/approve pay.

POCs

It is the responsibility of POCs to implement the defined segregation of duties policies and procedures based on profiles and roles as listed in Exhibit A.

POCs should establish access controls to enforce segregation of duties by:

- Implementing controls to ensure that policies are followed, once these policies and job descriptions have been developed.
- Using logical access controls, such as passwords and account roles, to restrict users to system access required to perform their duties.
- Using physical access controls, such as key cards, security guards, cipher locks, etc. to prevent unauthorized individuals from entering secured/sensitive work areas.

POCs should control personnel activities through formal operating procedures and supervision and review by:

- Implementing instructions to guide personnel in performing their duties; and,
- Monitoring personnel activities to ensure that policies and procedures are being followed.

Technical Team

Federal standards specify that key duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be segregated. This standard should also be applied to the authorization, testing and review of IT system changes. Technical staff duties should be segregated according to roles.

Segregation of Duties for Technical Staff:

- Programmers should not be responsible for moving programs into production or have access to production or have access to production libraries or data.
- Access to application system documentation should be restricted to authorized applications programming personnel.
- Access to production software libraries should be restricted to configuration management personnel.

- Persons other than authorized system administrators should not set up or operate systems in the production computer.

Regional/National Offices

Regional and National Offices are responsible for oversight and monitoring of SOPs, and for ensuring that agencies are in compliance with the requirements. Management reviews must be conducted to ensure that employees are performing their duties in accordance with the segregation of duties policies. A review of job functions, and segregation of duties will be included as part of the account re-certification process.

Exhibit A – System Profiles and Roles

The following system profiles were established based on segregation of duties.

Center Information System (CIS) – Profile Matrix

Job Corps center management should define standard Center Information System (CIS) profiles and incorporate them into the center's SOPs. Exhibit C provided by the Federal Information Systems Control Access Manual, includes sample technical job functions and job descriptions to illustrate segregation of duties.

Career Transition System (CTS) – Roles

- CT Manager
- CT Coordinator
- CT Specialist
- Center CTS Support Staff
- Regional Staff
- NTC Staff
- Other Support Staff

Electronic Property Management System (EPMS) – Roles

- Local Property Manager
- Regional Property Officer/National Property Contractor
- JCDC Property Officer
- Local Report –Read-only Access
- Regional Report – Read-only Access

Financial Management System (FMS) – Roles

- National Office
- Contractor
- Regional Office
- CCC Agency
- NTC

Job Corps Resource Library (JCRL) – Roles

- National Office
- Contractor
- Security Procurement Document Access
- Center
- OA Agency

- CTS Agency
- Regional Office
- NTC

Outreach and Admission Student Input System (OASIS) – Roles

- OA Counselor
- OA Manager
- Regional Staff
- National Call Center Staff

Survey Support System (S3) – Roles

- Survey Manager
- Survey Staff

IT Project Tracking System (IT Trax) – Roles

- Requestor
- JCDC Technical Team
- DOL Project Manager (National/Regional Staff)

Exhibit B – Job Corps Rules for Segregation of Duties

The following summarizes the key system access and job functions where segregation of duties is required:

System access where segregation of duties is required:

- No individual user should have access to all three student tracking applications -- OASIS, CTS, and CIS -- unless special authorization is obtained from the National or Regional Office. For example, the National Office authorizes an employee to have access to all three systems in order to conduct internal audits at Job Corps centers.

The following steps involved in processing transactions must remain segregated:

- Data entry and verification of data
- Data entry and its reconciliation to output
- Data entry and supervisory authorization functions (e.g., staff who enter leave requests should not also have the authorization to approve them).
- Employees who admit a student into the Job Corps program should not have access to modules in CIS, which would enable them to enter student pay information.
- Employees who enter student pay information must not authorize/approve pay.

IT functions where segregation of duties are required:

- There should be a separation of duties between Application Programmers, System Operations, Data Base Administrators, and Security.
- Application users cannot access the operating system or application software.
- Programmers should not approve or move programs into production.
- Only operations staff should set up and run production.

Note: In those instances where duties and system access and critical system functions cannot be fully segregated, mitigating controls must be established (at each location) as appropriate. Mitigating controls are additional procedures designed to reduce the risk of errors, irregularities or fraudulent activities. Procedures could include such controls as maintaining logs, monitoring staff activities, dual authorization requirements, and documented reviews of input/output.

Exhibit C – Sample Technical Job Functions and Job Descriptions

The table below illustrates segregation of duties. *Source: Federal Information Systems Control Access Manual (FISCAM)*

Job Functions	Job Descriptions
Information System (IS) Management	Includes the personnel who direct or manage the activities and staff of the IS department and its various organizational components.
Systems Design	The function of identifying and understanding user information needs and translating them into requirements document that is used to build a systems.
Application Programming	Involves the development and maintenance of programs for specific applications, such as payroll, inventory control, accounting, and mission support systems.
Systems Programming	Involves the development and maintenance of programs that form the systems software, such as operating systems, utilities, compilers, and security software.
Quality Assurance/Testing	The function that reviews and tests newly developed systems and modifications to determine whether they function as specified by the user and perform in accordance with functional specifications. Testing may also determine whether appropriate procedures, controls, and documentation have been developed and implemented before approval is granted to place the system into operation.

Library Management/Change Management	The function responsible for control over program and data files that are either kept on-line or are on tapes and disks that are loaded onto the computer as needed. Software programs are generally used to assist in the control of these files. This function also is often responsible for controlling documentation related to system software, application programs, and computer operations.
Computer Operations	The function responsible for performing the various tasks to operate the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems.
Production Control and Scheduling	The function responsible for monitoring the information into, through, and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is utilized in this task. An entity may have a separate data control group that is responsible for seeing that all data necessary for processing is present and that all output is complete and distributed properly. This group is generally also responsible for reconciling record counts and control totals submitted by users with similar counts and totals generated during processing.
Data Security	The function responsible for the development and administration of an entity's information security program. This includes development of security policies, procedures, and guidelines and the establishment and maintenance of a security awareness and education program for employees. The data security function is also concerned with the adequacy of access controls and service continuity procedures.

Data Administration	The function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the entity. Database administration is a narrower function concerned with the technical aspects of installing, maintaining, and using an entity's databases and database management systems.
Network Administration	The function responsible for maintaining a secure and reliable on-line communications network and serves as liaison with user departments to resolve network needs and problems.