

**IT Segregation of Duties Policy**

Version 1.0

**Document Key Information:**

|  |  |
| --- | --- |
| **Title:** |  |
| **Topic:** |  |
| **Classification:** |  |
| **Status:** |  |
| **Owner Department:** |  |
| **Document Approver:** |  |
| **Group/Local Scope:** |  |
| **Version:** |  |
| **Last Review Date:** |  |
| **Next Review Date:** |  |

**Document Change Control:**

To track reviews, updates and approvals actions related to the document

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** | **Date:** | **Change Description Summary** | **Change by:** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. Introduction 4](#_Toc114408806)

[2. Scope 4](#_Toc114408807)

[3. Deviations and Waivers 4](#_Toc114408808)

[4. Non-Compliance 4](#_Toc114408809)

[5. Principles of IT Segregation of Duties Policy 5](#_Toc114408810)

[6. General Guidelines 5](#_Toc114408811)

[7. Roles and Responsibilities 7](#_Toc114408812)

[8. Operating Systems and Infrastructure 8](#_Toc114408813)

[9. Privileged Accounts 8](#_Toc114408814)

[10. Production Environment 9](#_Toc114408815)

[11. Disaster Recovery and Business Continuity Environment 10](#_Toc114408816)

[12. Separation of Development and Operational facilities 10](#_Toc114408817)

[13. Development and Test Environments 10](#_Toc114408818)

[14. Program Source Code 11](#_Toc114408819)

[15. Live System Data 11](#_Toc114408820)

1. Introduction

The purpose of this policy is to ensure that system controls are implemented properly as per the company policy and applicable legislation. 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. Segregation of duties involves breaking down tasks that might reasonably be completed by a single individual into multiple tasks so that no one person is solely in control.

1. Scope

This policy covers all the System components (‘IS’ or IT’) environment and Information/IS Assets owned and operated by [COMPANY NAME] or operated by any third party on behalf of [COMPANY NAME].

This policy applies to all users of information assets including employees (whether permanent, fixed term, consultancy or other) and employees of third-party service providers, regardless of geographic location.

This policy communicates the minimum requirements for the segregation of duties across [COMPANY NAME] and by extension, across Cloud services (including IaaS, PaaS, and SaaS) associated to [COMPANY NAME] and any of its offices.

This policy applies to all Information Technology activities that have a direct or indirect relation with Cyber and Information Security controls.

1. Deviations and Waivers

All staff must comply with this policy. Failure to do so may subject [COMPANY NAME], its staff or any third-party contractors to civil and/or criminal liability.

If an office or department cannot follow or comply with any of the requirements detailed within this policy due to technical and operational limitations, a prior waiver must be sought from Risk Committee.

1. Non-Compliance

Employees must report any suspected or confirmed violations of this policy to Cyber and Information Security Department. Actions that are considered to be non-compliant or a breach of [COMPANY NAME] security policies, standards and procedures will be reviewed on an individual basis. Breaches may result in disciplinary action being undertaken and may lead to termination of employment or criminal charges.

1. Principles of IT Segregation of Duties Policy

This policy reflects the following principles:

* 1. **Segregation of Duties**: Segregation of duties involves breaking down tasks that might reasonably be completed by a single individual into multiple tasks so that no one person is solely in control.
	2. **Need to Know**: A method of isolating information based on a user’s need to have access to it to perform his/her job.
	3. **Need to Use**: A method of isolating information resources and facilities (e.g., IT equipment, applications, procedures, secure rooms, etc.) based on a user’s need to have access to perform their job but no more
	4. **Least Privileges**: A method of isolating information resources and facilities (e.g., IT equipment, applications, procedures, secure rooms, etc.) based on a user’s need to have access to perform their job but no more.
	5. **Default Deny**: Everything is generally forbidden unless expressly authorized.
	6. **Confidential**: All information and data at [COMPANY NAME] is considered confidential and for Internal use only by default unless expressly classified and labelled otherwise by the owner. The criticality of information assets must be considered and documented using the rules established in the asset classification and controls in the Information Security Policy
	7. **Secure at All Times**: Data must be secured at all times and locations, and in any of the three data states: in Use, in Transit and at Rest.
	8. **Ownership of Information Assets**: Owners must be identified for all systems, services and assets used in [COMPANY NAME]. The execution of specific security controls may be delegated by the owner as appropriate, but the owner remains ultimately accountable for the proper protection of the information assets.
	9. **System Owner**: The term “System Owner” identifies an individual that has approved management responsibility for controlling the production, development, maintenance, use or security of systems, information assets, services and/or assets under his/her supervision.
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, The change implementer should not approve his/her own request.
* 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. Therefore, [COMPANY NAME] IT and Information Security team should work together to apply the Segregation of Duties concept in all IT and Security related activities.
* Inadequate segregation of duties increases the risk that wrong or fraudulent activities could be performed, 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 risk associated with its activities.
* Segregation of duties must be divided among major operating and programming activities, including duties performed by users, IT staff, and Information Security staff.
* Any activity that could result in fraud or misuse of [COMPANY NAME] information or systems must have mitigating controls for separation of duties, or the implementation of controls to detect fraud or misuse. In addition, the following duties must be performed by separate groups of employees:
* IT Management
* Software development
* Software testing
* Program promotion/change management librarian
* Systems operations / daily administration
* Helpdesk/support
* Network management
* IST (Information Security Team).
* Access and use of the Information Assets must be authorized by the System Owner and must follow the Need-to-Know and Need-to-Use principles.
* Access and use of [COMPANY NAME] resources on the network must be strictly controlled to prevent unauthorized access and must follow the Default-Deny and Need-to-Use principles.
* Access or use of the Information Assets must be authorized by the System Owner and must follow the Need-to-Know and Need-to-Use principles.
* Appropriate Access Control Mechanisms must be implemented to enforce a default deny access from non-[COMPANY NAME] assets and from unauthorized [COMPANY NAME] assets. Default deny means the action is restricted by default unless granted by an approved request.
* Need to use means a valid and legitimate business justification to take a specific action. This justification needs to be detailed in the change request for review and future reference purposes.
* All approved programs and mechanisms used to access live data must follow the least privilege principle. The minimum required privilege needs to be granted only.
1. Roles and Responsibilities
	1. **Management:**

Segregate duties and establish related procedures by:

* + Analysing operations.
	+ Identifying duties.
	+ Assigning these duties to different organizational units or individuals.
	1. **Users:**

Users are responsible for ensuring that they follow standard operating procedures as defined by management and Segregation of Duties policy.

* 1. **Cyber and Information Security:**

It is the responsibility of Cyber and Information Security to test that the requirements of this Segregation of Duties policy are adopted by IT wherever relevant to Information Security including:

* + Implementing controls to ensure that the policy is followed.
	+ 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 High Secure Areas.
	+ Review and Approve IT changes and requests in line with this policy.
	+ Participate in defining, reviewing and approving IT policies, standards and procedures to ensure the alignment with Segregation of Duties policy.
	+ Review and approve baseline configuration standards prepared and performed by IT team.
	1. **Information Technology:**
	+ This policy applies to the authorization, testing and review of IT system changes. Technical staff duties should be segregated according to roles.
	+ 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 environment.
	1. **Information Owner:**
	+ Information Owners are responsible for reviewing system privileges to identify segregation of duties conflicts and ensure that access rights match those that have been approved and revoke inappropriate access rights. Reviews must be performed due to the ever-changing business environment and the importance of the data. It is the responsibility of system administrators to ensure that Information Owners are provided with the proper reports to review current user access.
1. Operating Systems and Infrastructure
* Access to system infrastructure (e.g., operating systems, database management system, network devices, security devices, etc.) commands is to be restricted to those privileged users who are authorized by the IT and Information Security to perform systems, network, security and database administration functions.
* End users are not allowed to have local privileged accounts over computer devices.
* The allocation and use of privileged accounts must be controlled by IT, Information Security and, where applicable, System Owners.
* Privileged users must neither use their privileged accounts to perform their normal day-to-day activities (e.g. access to email, accessing the Internet etc.) or for other purposes other than the approved administration activities.
* Privileged users must not grant their normal account with an admin privilege.
* Privileged users must not use their privileged accounts to gain access for or grant access to other individuals without following the approved change management workflow process for user management
* All access and use of operating systems’ privileged commands must be restricted, logged, and monitored independently by Information Security or any other delegated party.

1. Privileged Accounts
* Emergency accounts must only be used under controlled access when normal operational and/or administrative access is not available. Access to these accounts requires approval from the Head of IT and Information Security.
* Access to privileged accounts must be restricted, centrally logged, and monitored independently by Information Security or any other delegated party.
* If a privileged account needs to have remote access such access must be approved by the Head of IT and Head and Information Security and must be performed from a well-secured workstation that meets [COMPANY NAME] security standards and system hardening.
* Only authorized users should access, or attempt to access, a privileged account. An electronic access control list of users authorized to access each service account must be maintained by the Head of IT and validated by Information Security periodically.
* Any user not expressly listed as an authorized user of a privileged account is an unauthorized user of the account and is totally forbidden from accessing or attempting to access the privileged account.
* The owner(s) of the privileged accounts are responsible for monitoring the activities performed with the privileged account with the support of Information Security.
1. Production Environment
* All the requirements mentioned in this document are applicable to the Production environment. Any exceptions must be clearly documented and approved by the System Owners, Heads of IT, and Information Security.
* Access to Production Environment must only be through approved mechanisms such as Jump Server, Multi-Factor Authentication, SSH clients and Secure RDP sessions.
* All access to Production Environment must be logged, monitored, and reviewed either using log monitoring solution. As a minimum the logs should capture: User IDs, date, time, actions, commands, and modified parameters.
* All approved access to Production Environment must follow the Least Privileges principle.
* In case of using Privileges Access Management solution for Production Environment access, The system must be configured to provide only access to essential capabilities and to specifically restrict or disable access to functions, services and commands that are not needed.
* Access to Production Environment shall be based on its default classification (if not classified by the owner) and handling instruction as documented and approved by the System Owner.
* Production Environment Backup data must not be restored to Test and Development environments.

1. Disaster Recovery and Business Continuity Environment
* Disaster recovery and business continuity environments must enforce the same level of security and segregation of duties as in production. Any exceptions must be clearly documented in the Disaster Recovery and Business Continuity Plans and approved by the System Owners, Heads of IT, and Information Security.
* Access controls at the application, infrastructure level (e.g., perimeter defence) and support level (e.g., data leakage prevention, internet access, etc.) must not be overshadowed or ignored during recovery planning and post recovery operations.
1. Separation of Development and Operational facilities
* Separately controlled environments must exist for development, testing, and production. Development and production software should run on separate machines wherever possible. If separate machines are not feasible, then the production and development software should run on different domains or directories in a manner such that appropriate access control mechanisms can be implemented to restrict access of software developers and testers to the production environment.
* The production environment is where the production executable code for an application must reside. Only an authorized change management librarian must have “write” access to these executables.
* Compilers of other system development tools must not be installed on production machines. If a compiler is necessary on a production machine, the access and execution rights must be strictly controlled. All codes must be pre-compiled before moving into the production environment.
* The test environment must be kept separate from the production environment by using logical controls to help follow the Segregation of Duties.
* Production data (live PAN) should not be used for testing purposes until it has been sanitized/scrambled/masked.
* Test data should be removed before production become active.
1. Development and Test Environments
* Access to development environments must be restricted to the employees responsible for development. Access to test environments must be restricted to project and testing teams.
* If access to the test environment involves access to production data, this data must be masked, anonymized, tokenized, or dummy data with access approval obtained from the System Owner. If this is not possible, appropriate controls and monitoring over the production data should be approved by the Heads of IT and Cyber and Information Security and implemented.
1. Program Source Code
* Access to program source code should be restricted to the employees performing the software librarian role and with release and deployment management responsibilities.
* Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) should be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property.
1. Live System Data
* Access to live data must only be through approved programs (including scripts, batches, stored procedures, middleware interfaces, and any other types of job control languages) that are documented and securely stored in application libraries (i.e., operating system and database libraries).
* Direct access to live data in case of emergency must be clearly documented and approved by the System Owner, Head of Cyber and Information Security and Head of IT. If they cannot be reached, then the approval must be obtained retrospectively and documented as such.
* All direct access to live data must be logged, monitored, and reviewed either using the operating system or database audit logging capabilities or a database activity monitoring software. As a minimum the logs should capture: User IDs, commands, and tables and fields modified.
* All approved programs and mechanisms used to access live data must follow the Least Privileges principle.
* Infrastructure components must be configured to provide only access to essential capabilities and to specifically restrict or disable access to functions, services, ports, and protocols that are not needed by the system and support programs.
* Approved access privileges to data in Use must also be maintained when data is in Transit and at Rest.
* If data is not classified, it must be considered as Confidential and for Internal use only by default.
* Access to live data shall be based on its default classification (if not classified by the owner) and handling instruction as documented and approved by the System Owner.
* Access to other employee’s files, folders or email, including the files and folders of staff that have left the company, must be approved by Human Resources, Cyber and Information Security and the relevant Head of Department.
* Access to backup software and backup media must be restricted to employees with clearly defined and assigned backup management responsibilities.
* Data must not be restored without prior approval. It must be requested using an approval workflow and include a change, incident, or service request ticket number.
* All data restoration requests must be authorized by the Head of Department, Head of Cyber and Information Security and must be granted based on justified business reasons. System Owner must approve as well if involving their Information Asset.
* Access to encryption keys must be restricted to appropriated authorized personal.
* Where two or more authorized employees share part of an encryption key, access should be segregated to ensure that no one employee has access to the key, as anyone having access to the full key is able to decrypt all information being encrypted with it. Heads of Department should have appropriate oversight, management, and controls of the encryption keys to ensure access to the data is available when required.