User Access Management Procedure

KG Invicta Services (KGiS)

[Ref: ISM-PLC-DOC-06]
[Ver: 1.0]
[05th April 2023]
[Classification: Internal]

+91 422 4419999

KGiS
o 365, KG Invicta Services Private Limited KGiS Campus, Thudiyalur Road, Saravanampatti, Coimbatore - 641035, India

www.kginvicta.com

Statement of Confidentiality

This document contains confidential and proprietary information of KG Invicta Services Private Limited (KGiS). It is furnished for KGiS internal use and purpose only. Except with a prior written permission of KGiS, this document and the information contained herein may not be published, disclosed, or used for any other purpose. This document is reviewed at least annually.

Copyright and Intellectual Property

a. KGiS logo are registered marks of KG Invicta Services Private Limited.

b.

Table of Contents

1 Document Control

1.1 Document Owner and Approval

KGiS's Information Security Office (ISO) is the accountable owner of this procedure. The ISO is responsible for ensuring that this document is reviewed periodically by the relevant stakeholders in line with the review requirements of the Information Security Management System (ISMS).

A current version of this document is available to all KGiS members at the corporate Intranet and is published on 05th April 2023.

This procedure document was approved by the Head of ICT on 05th April 2023 and met the required Documentation Quality Standard and is issued on a version-controlled basis under the signature.

Name: Shanmugam C

Designation: GM - ICT

Signature: Date: 05th May 2023

1.2 Amendment History Record

Version	Description of Change / Action	Resource	Date
1.a	New draft baseline of ISMS procedure	Harikrishnan P	04th May 2023
1.0	Verified and Approved By	Shanmugam Chinnasamy	05th May 2023

1.3 Cross References

All reference documents available in – Shared Folder
ISO 27001– Information technology – Security Techniques – Information security – Requirements
ISO 27002 – Information technology – Security techniques – Code of practice

1.4 Document Sign off and Distribution

Name	Designation	Signature	Version	Date
Shanmugam Chinnasamy	GM- ICT		1.0	05th May 2023

Document Distributed for Internal Approval.

Stakeholder	Date
All Head of Departments and Departments	

2 Definitions & Glossary

Term	Definition
Confidentiality	Prevention of unauthorized access by people, resources, and processes to information.
Integrity	Prevention of intentional or accidental unauthorized changes to information.
Availability	Assurance that information is accessible by authorized users whenever needed.
Authentication	Authentication is the act of verifying a claim of identity. It is usually one or more of the following: (1) Something you know (a password) (2) Something you have (a smart card or certificate) and (3) Something you are (fingerprint or retinal pattern)
Authorization	Authorization determines what a subject can do on the system. Authorization happens right after identification and authentication.
Information System Owner	An individual or a group which is assigned with the responsibility to define the technical functionality of information systems in order to accomplish the expected business objective and user requirements including the implementation of appropriate security safeguards.
System Administrator	An individual or group of employees responsible for the maintenance, operation, and administration of the information systems
IS Officer	Information Security Officer
ISO	International Organization for Standardization
Information	Information is an asset which can exist in many forms such as printed or written on paper, stored electronically, transmitted by post or by using electronic means, or spoken conversation and has a value to an organization.
Information Security	The act of protecting information that may exist in any form mentioned above from unauthorized access, use, disclosure, disruption, modification or destruction, with the objective of ensuring business continuity, minimizing business risk, and maximizing return on investment and business opportunities.
Users	User is an individual, including all the employees of KGiS and vendor or third-party contractor, who has access to the information and information processing facilities of KGiS ICT and uses it for his/her day-to-day activities.

Intellectual Property	Intellectual Property refers to any creations that are legally protected. Intellectual property includes copyrights, trademarks, trade names, and logos of KGiS ICT
Credentials	User ID, Passwords or any other official identification that confirms somebody's position or status
Access Control	Access control is a mechanism to enable authorized people to access KGiS ICT's resources (logical and physical) while preventing unauthorized people from doing the same.

3 About the Document

3.1 Introduction

The User Access Management Procedure is a fundamental component of an organization's information security framework. It provides a structured and systematic approach for managing user access to critical systems, networks, and data. User access management ensures that authorized individuals have appropriate access privileges while preventing unauthorized access and protecting sensitive information from misuse or unauthorized disclosure.

This introduction aims to provide an overview of the User Access Management Procedure and its significance in maintaining the confidentiality, integrity, and availability of organizational resources. It outlines the objectives, scope, and benefits of implementing a robust user access management process, emphasizing the importance of controlling user privileges, enforcing least privilege principles, and maintaining an audit trail of access activities. By establishing effective user access controls, organizations can mitigate the risk of unauthorized access, reduce insider threats, and ensure compliance with regulatory requirements.

Furthermore, this introduction highlights the importance of user access management in fostering a secure and productive work environment. It emphasizes the need for clear policies, role-based access controls, regular access reviews, and user provisioning/deprovisioning processes. By implementing a well-defined user access management procedure, organizations can enhance security, streamline access administration, and protect sensitive information from unauthorized disclosure or manipulation.

3.2 Objective

The objective of this procedure is to enables KGiS and maintain a secure and controlled environment, protect sensitive information, comply with regulations, and minimize the risk of unauthorized access. It enables organizations to effectively manage user access, mitigate security threats, and ensure the integrity and confidentiality of their resources and data.

3.3 Scope

This procedure applies to all information assets management owned or managed by the KGiS ICT staff (permanent, contract employees, and students), and external parties (contractors, consultants, vendors, suppliers, partners and customers)

3.4 Roles and Responsibilities

- Head of ICT is responsible to review and approve this procedure and to ensure that it reflects the current requirements.
- Head of ICT is responsible for developing, implementing, maintaining and enforcing the procedure.
- Internal Audit Team is responsible for conducting regular audits to ensure compliance to this procedure.

- Respective Departmental managers are responsible for reviewing and approving access provisioning and revocation requests.
- The System Administrators are responsible for following the defined procedures during provisioning and revoking access to the Information systems.
- Information Security Officer is responsible for conducting periodic review of access rights and privileges on KGiS information processing systems and facilities.

4 Procedure

The processes that need to be followed for the effective implementation and management of this procedure are explained in this section.

4.1 Access Provisioning

- Once new employees enter the organization, access is provided for them on active directory by ICT team with the approval from HR department. Further application-level access is provided through the process described herein.
- All employees who require access to information asset owned and managed by the ICT Department should raise a request through email or Service Desk tool.
- The request can be used to manage access rights to the following (but not limited to):
    - Access to Domain/applications/databases;
    - Access to the Email/Internet facilities;
    - Access to Files and Folders;
    - Wireless Network Access, Remote Access;
    - Administrative access to Server Console, Network Device Console etc; and.
    - Extending lifetime of a user account.
    - Assigning/modifying/revoking Privileges of a User Account
- Access provisioning request with respect to information asset owned and managed by the ICT Department should be initiated for the following cases, but not limited to:
    - New employment;
    - Employees getting transferred to a different section/department/division;
    - Employees being promoted/ demoted;
    - New assignment of job responsibilities; and
    - Any other business requirements.
- The user should raise a request in service desk tool with the required details and submit it to the respective Service Owner for approval.
- The respective Service Owner is responsible for reviewing and approving the request.
- The respective Service Owner should verify the validity period for the requested access. Validity period should be defined mandatorily while provisioning access to third-party users such as vendors and partners.
- The respective Service Owner/ authorized departmental users may initiate the request by him/her only in cases where it requires to provision access and make arrangements before an employee joins the services of KGiS.

- The request, based on the type of access requested, should then be forwarded to the concerned section within ICT Department for validation and further completion of the process.
- The system owner/ respective Section Head should review the requested access for compliance with KGiS policies and procedure or security requirements.
- If the request is a privileged access request, Service Owner/ Head of sections should forward it to the ISO and Head of IT for review and approval. If disapproved, the ISO may communicate the reason to the Service Owner and the respective departmental manager.
- If the request is a standard access request, the system owner may directly designate the request to the system administrator after proposal approval process.
- The system administrator should then configure the system to provision the requested access. The corresponding Service request ticket should be followed while provisioning the access rights. The system administrator should follow any applicable security policies, procedures and standards during the process.
- On successfully completing the request, the system administrator should notify the user and close the service desk ticket.
- The list of services accounts or generic accounts owner should be identified& documented by respective systems administrators.
- If a user forgets the password, Local IT is authorized to reset the password after having the confirmation of the user's authenticity from HR for staff or from student services department for students. Automatic password reset options are available for users through self-service portal.

4.2 Removal of User

The following steps should be followed for revocation of access rights from information processing systems and facilities owned and managed by the KGiS ICT Department. Revocation of access rights may be initiated in any of the following cases but not limited to:

- Employee resignation.
- Employee being terminated.
- Third-party users (such as vendors and partners) completing their engagement.
- Employee getting transferred to a different section/department/division (internal transfer)
- Employee job or role change.
- Employee being promoted/ demoted.
- Employee has been on prolonged leave of absence.

- If the employee is resigning/getting terminated/transferred from the organization, HR should initiate the Access revocation request to the ICT Department via Email/Service request.
- The Respective Departmental Managers should verify the details provided by the in the access revocation request.
- The Respective Departmental Managers himself/herself should initiate the access revocation request in the following cases:
    - Employee's contract is terminated abruptly on disciplinary grounds.
    - Employee has been on prolonged leave of absence.

4.3 Revocation – Logical Access

- In case of Employee resignation/termination/transfer, Line Manager should verify the Exit clearance in terms of access rights to be revoked, assets under possession of the user, and completion of all his/her duties etc.
- The request, based on the type of access revocation, should then be forwarded to the Service Owner for validation and completion.
- Upon validating the request, the Service Owner may designate the request to the system administrator.
- The system administrator should then disable the assigned access rights and privilege on the last working day of employee. The corresponding workflow ticket should be followed while revoking the access rights. The system administrator should follow any applicable security policies, procedures and standards during the process.
- On successfully completing of the request, the system administrator should notify the Service Owner, the Departmental Manager and close the service desk ticket.

4.4 Privilege Management

- Privileges associated with operating systems, databases, networks and applications should be identified and allocated based on the approval by relevant Departmental Heads/Service Owners.
- Privileges should be allocated and controlled on a need-to-know basis. Access requests shall be approved by Service Owners and Head of ICT and should be executed by the system/application administrator.
- Formal records of all privileged access rights or authorizations shall be maintained.

4.5 Review of Access Rights

- User accounts shall be reviewed every Six months to verify authenticity of existing user list.
- Privileged accounts (such as administrator accounts or other accounts that can override access controls) should be reviewed at least every quarter, and any changes should be logged.
- Information Security Officer should request HR department to provide with the list of employees in each section/department along with their designation roles on a monthly basis for employee exit review.
- IS Officer shall review the employee exit list with the date of revocation and last day of working.
- Upon review, IS Officer should identify any instances of following and share the report with the service owners:
    - Redundant / Dormant / Orphaned / Expired accounts
    - Accounts which are active even after the requested validity period
- Upon review, the IS Officer should identify any unused account, and any other security concerns, and share the report with the concerned department.

4.6 Roles and Responsibilities Matrix

Roles/ Responsibilities	End User/HR Department	User Department	Service Owner	System Administrator	Head of ICT
Request	R, A	R, A			
Access Provisioning– Logical Access	R	R,A,I	R,A,I	R,I	R
Access revocation – Logical Access		R,A,I	I	R, C,I	R,I

R Responsibility – The personnel who is responsible for performing the task.

A Accountability – The personnel who is accountable for the process or data.

C Consulted – The personnel who provide opinions or suggestions.

I Informed – The personnel who should be informed with the progress and updates.