User Access Request Procedure

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Procedure Statements 4

2.1 Roles and Responsibilities 4

2.2 Access to Network Folders 4

2.3 Access to IT Equipment 4

2.4 Returning IT Equipment 4

3. User Registration Procedures 5

3.1 General Access Request 5

3.2 Change of User Requirements 5

3.3 Change of Password 5

3.4 Removal of Users 5

3.5 Privilege Users 5

4. Review of user Access Rights 6

5. Procedure Compliance & Enforcement 7

5.1 Compliance Measures 7

5.2 Enforcement 7

6. Glossary / Acronyms 8

6.1 Glossary / Acronyms 8

7. Document Management 9

7.1 Document Revision Log 9

7.2 Document Ownership 9

7.3 Document Coordinator 9

7.4 Document Approvers 9

7.5 Distribution 9

# Introduction

## Document Definition

This document is a Procedure.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Objective

The User Access Management Procedure defines the procedures in place for granting, modifying, removing and reviewing user access privileges to XXXX systems and applications in order to protect the privacy, security and confidentiality of XXXX information assets and systems.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This procedure applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant procedure statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This procedure applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Procedure Statements

## Roles and Responsibilities

* User – this is the staff member who requires access to data/systems.
* Line Manager – this is the manager who is directly responsible for the user.
* Data Owner – this is the staff member who is responsible for the data. The data owner carries out regular risk assessments and should hold a list of who has access to the data.
* IT Helpdesk – System administrators who oversee granting logical access to users on the system.

## Access to Network Folders

Staff who have access to a specific network drive do not necessarily require access to all files that are stored on that drive. When a request is raised for a new user on helpdesk portal or through mail, the line manager must state all files that the staff member requires access to and only for the files listed will access be given.

## Access to IT Equipment

To receive mobile computing IT equipment including laptops and mobile phones a request must be made on the helpdesk portal or a mail sent by the line manager. IT will then look to allocate an existing equipment to the user, if there is a need for new equipment IT will work with the line manager in relation to cost and requirements and get the necessary approvals from management

## Returning IT Equipment

All mobile computing devices must be retrieved by the line manager from the staff member on termination of employment or change of job roles where the equipment is no longer required. The device must be returned to IT department where the device can be securely stored and reallocated appropriately. If the equipment was purchased by the Team’s budget the equipment can be reallocated to the Team by IT

# User Registration Procedures

## General Access Request

The following steps must be followed to obtain access to XXXX systems, network access, applications, equipment, folders and any databases:

* The user must send the request through the helpdesk portal and approved by the line manager ([https://XXXXhelpdesk.sdpondemand.manageengine.com/app/itdesk/HomePage.do](https://zbukhelpdesk.sdpondemand.manageengine.com/app/itdesk/HomePage.do).)
* The user must pick the system owner to approve the request on the help desk portal.
* The system owner gets the request on the helpdesk and approves.
* The Head of IT can then allow access to the required data if the request has been approved at all authorisation levels.

For new users this process can be completed prior to their employment start date to ensure that the data can be accessed on the date they start the position. If the user has been given a start date this must be entered on the form so that access will start on the required date

## Change of User Requirements

Changed requirements will normally relate to an alteration to the applications used but may also involve network access.

1. User makes a request must in writing (e-mail or helpdesk portal) and approved by the line manager
2. The request is approved by the system owner
3. Head of IT receives the request and direct that the necessary changes be made after reviewing that the request has been appropriately made
4. IT responds to user that the request has been treated.

## Change of Password

Where a user has forgotten his/her password or locked out of the system, the helpdesk is authorised to issue a replacement or unlock the user

1. Line manager or colleague of affected user logs the request on helpdesk portal or send an email to helpdesk stating the affected username and request for password request
2. Helpdesk will Issue a temporary, single use, password which will require the user to set up a formal password and send this to the requesting staff
3. Requesting staff gives the password to the affected user to log in and a change the password

## Removal of Users

As soon as an individual leaves the XXXX’s employment, all his/her system logons must be revoked.

1. HR will inform IT Helpdesk of all leavers and their date of leaving either through mail or helpdesk portal.
2. IT will remove the users from all applicable systems and send a confirmation to HR that it has been done

## Privilege Users

Special privileges are those which allow the system manager or systems programmers to access sensitive areas (for example, passwords, production databases). The unnecessary allocation and

use of special privileges is often found to be a major contributing factor to the vulnerability of

systems that have been breached

Privileged access must be authorised by the Head IT, the minimum information required to grant this access must include:

**Name of applicant:**

**Job Title:**

**Systems Login Name Access Level Reason**

**Access required: From date:**

**To date:**

**System owner name:**

**System owner’s comments:**

1. User log the request through the helpdesk portal or through helpdesk mail including all the above information
2. Helpdesk sends the request to Head IT for approval
3. After the request have been duly approved, IT creates the user with the required privileges
4. The user is informed by helpdesk of the login details

# Review of user Access Rights

Each system owner will carry out a user review of their applications, this review is to be done quarterly. The results of the reviews are kept in a sharepoint folder and Head IT and ISO ensures all the reviews are completed and uploaded.

Any lapsed or unwanted logons, which are identified, will be disabled immediately and will be

deleted unless positively reconfirmed.

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
| ISO | Information Security Officer |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Procedure is owned by the YYYY

## Document Coordinator

This Procedure is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Distribution

* Distribution is to all staff