

STANDARD OPERATING PROCEDURE

IT Onboarding and Access Management

Procedure for creating, changing and removing user access

DOCUMENT NO.

SOP-IT-007

VERSION

2.0

EFFECTIVE DATE

1 February 2026

Document Control

Document title	IT Onboarding and Access Management
Document number	SOP-IT-007
Version	2.0
Effective date	1 February 2026
Owner	IT Manager
Approved by	Chief Technology Officer
Review cycle	Every 12 months or when the process changes

Revision History

Version	Date	Description of change	Approved by
1.0	Apr 2024	First issue	CTO
2.0	Feb 2026	Added quarterly access reviews	CTO

Uncontrolled when printed. Always check the shared drive for the latest version.

Contents

Purpose.....

Scope.....

Definitions.....

Roles and Responsibilities.....

Procedure.....

New Joiners.....

Role Changes.....

Leavers.....

Quarterly Access Review.....

RACI Matrix.....

Records and Forms.....

3

3

3

3

4

4

4

4

4

4

5

Performance Indicators.....	5
Appendix A: Access Request Form.....	5
Acknowledgement.....	5

Purpose

To ensure that employees receive the right access on time and that access is removed promptly when no longer required, protecting company and client data.

Scope

Applies to all employees, interns and contractors and to all company systems, devices and cloud services.

Definitions

Term	Definition
Least privilege	Giving only the access needed to do a job
MFA	Multi-factor authentication
Access review	Periodic check that access is still appropriate

Roles and Responsibilities

Role	Responsibilities
HR	Raises joiner, mover and leaver requests
Manager	Approves access for team members
IT team	Creates, changes and removes access
System owner	Approves access to sensitive systems

Procedure

New Joiners

1. HR raises a joiner request five working days before the start date.
2. Manager confirms the role and required systems.
3. IT creates accounts with MFA enabled and prepares the laptop.
4. On day one, IT hands over the device and explains security basics.

Role Changes

5. Manager raises a change request.
6. IT adds new access and removes access no longer needed.
7. System owner approves sensitive access.

Leavers

8. HR raises a leaver request with the last working day.
9. IT disables accounts at the end of the last day.
10. Device is collected, wiped and logged.

Urgent removal

For involuntary exits, access is removed immediately on HR request.

Quarterly Access Review

11. IT exports user lists from key systems.
12. Managers confirm or remove access within 10 working days.
13. Results are recorded and exceptions resolved.

RACI Matrix

R = Responsible, A = Accountable, C = Consulted, I = Informed.

Activity	HR	Manager	IT	System owner
Joiner request	R	A	I	—
Create access	I	C	R	A
Remove access	R	I	R	I
Access review	I	R	A	C

Records and Forms

Record / form	Kept by	Retention
Access requests	IT ticketing system	3 years
Access review results	IT Manager	3 years
Asset register	IT team	Life of asset

Performance Indicators

Indicator	Target	Frequency
Accounts ready on day one	98%	Monthly
Leaver access removed same day	100%	Monthly
Access review completion	100%	Quarterly

Appendix A: Access Request Form

Employee name and ID	
Role	
Systems requested	
Access level	
Manager approval	
System owner approval	

Prepared by

Checked by

Acknowledgement

I confirm that I have read and understood this document and will follow it.

Name and signature

Date