User access request and access review

Process Definition Document (PDD): template and worked example

Example company (fictional): Selwyn Hartley Asset Management Ltd, an investment manager in Edinburgh, United Kingdom (about 650 employees and 45 business systems).

Document control

Field	Value
Process name	User access request and access review
Process owner	[Name, role]
Prepared by	[Name]
Reviewed by	[Names of the people who do the work]
Approved by	[Name, date]
Version	1.0 (as-is)
Status	Draft

How to use this template

This is a complete process definition document (PDD) for user access management, also called the access request process, user provisioning procedure, joiner mover leaver process or periodic user access review (access recertification). It describes how an employee asks for access to a system, how it is approved by the line manager and the system owner, how segregation of duties is checked, how access is provisioned, and how every system owner reviews who has access each quarter and removes what is no longer needed. The organisation is a fictional investment manager, so the roles, systems and numbers are realistic but invented.

Use it as a starting point. Replace the company details, keep the sections, and walk through each step with the people who request, approve, grant and review access. Most teams change the review frequency, the list of systems in scope and the segregation of duties rules. If your joiner process is already covered by an onboarding procedure, link to it from step 1. The template describes a control process and does not claim compliance with ISO 27001, SOX or any other standard. It must be adapted to your own risk rules and to what your auditors expect.

- Replace the company, the identity platform and the HR system with yours. If you do not use SailPoint, name the spreadsheet or report that holds the extract and the review decisions.
- Decide which systems are in scope and how often each is reviewed. High-risk systems and privileged access are often reviewed quarterly and others twice a year.
- Write your own segregation of duties matrix. Start with the five or ten conflicts that matter in your business, such as creating and approving payments.
- Give roles names that a manager understands, and pre-approve the low-risk ones so that system owners only decide the rest.
- Connect the HR system to the identity platform if you can. The leaver delay is usually the biggest single improvement.
- Agree with your auditors what evidence they need. Name, date, decision and removal reference per entitlement is a common minimum, but they decide.
- Check the percentages against a quarter of real data, especially the late reviews and the revocation rate.

1. Purpose and scope

This procedure describes how Selwyn Hartley Asset Management gives people the access they need to do their job and no more, and how it proves that this stays true over time. It gives requesters, managers, system owners, administrators and compliance one shared description of who approves and grants access, how conflicts of duty are caught, how access is reviewed and how leavers and movers lose access, so that every entitlement has an approver, a reason and a recent review.

In scope

- Requests for access to business systems, shared folders and privileged roles
- Line manager and system owner approval
- Segregation of duties check against a conflict matrix
- Provisioning and recording of access in the identity platform
- Quarterly access review by system owners and line managers
- Removal of access for leavers and for staff who change roles
- Evidence for internal and external audit

Out of scope

- Creation of the identity and standard joiner bundle, which follows the new joiner process
- Access to the building and to trading floor hardware, which is managed by facilities
- Break-glass emergency accounts, which have their own sealed-envelope procedure
- Customer portal accounts, which are managed by the client service team

2. Process at a glance

Item	Description
Trigger	An employee, contractor or manager needs access to a system, or a quarter ends, or HR reports that someone is leaving or changing role.
Starts when	The requester submits an access request in ServiceNow, or compliance launches the quarterly review campaign.
Ends when	Access is provisioned and recorded, or the review campaign is complete and the evidence pack is filed.
Inputs	Access request with system, role and reason, Role catalogue and segregation of duties matrix, Entitlement extracts from each system, HR leaver and mover feed, Prior review results
Outputs	Approved and provisioned access with an audit trail, Segregation of duties decisions and compensating controls, Signed-off review results per system, Removal confirmations, Quarterly evidence pack
Volume	About 380 access requests a month. Each quarter about 22,000 entitlements across 45 systems are reviewed, and about 60 leavers and 40 movers a month are processed.
Working hours	Requests accepted at any time and provisioned within 2 working days. Review campaigns open in the first week of each quarter and run for 15 working days.

3. Roles and responsibilities

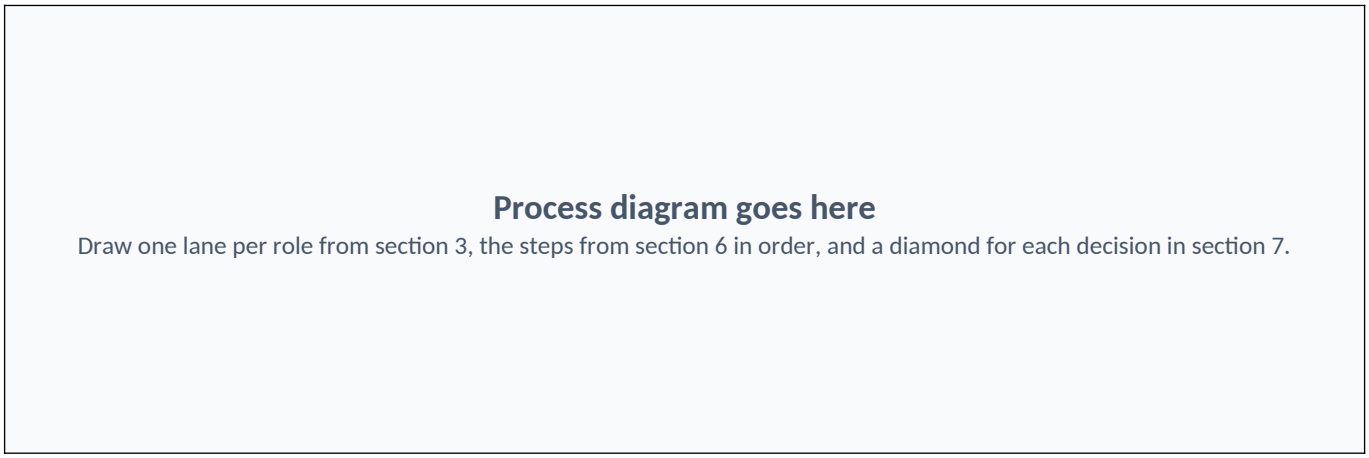
Role	Responsibilities
Requester	The employee or contractor who needs access, or a manager asking on behalf of a new team member. States the system, the role and the business reason.
Line Manager	Confirms that the person needs the access for their job. Also reviews the access of their direct reports each quarter and confirms the access for movers.
System Owner	The business owner of a system. Approves the level of access, defines which roles exist, and reviews every entitlement on the system each quarter.

Role	Responsibilities
Access Administrator	The IT identity team member who provisions and removes access in the target systems and records it.
Compliance Analyst	Checks requests against the segregation of duties matrix, approves exceptions with a compensating control, runs the quarterly review, chases late reviewers and builds the evidence pack.
HR Operations	Sends the leaver and mover notices from the HR system, with the effective date, on the day the decision is made.
Internal Audit	Tests a sample of requests, reviews and removals each year and reports exceptions to the audit committee.

4. Systems

- ServiceNow: access request catalogue, approvals and tickets
- Microsoft Entra ID: identities, groups and application assignments
- SailPoint IdentityIQ: entitlement extracts, review campaigns and certification records
- Workday: employee records, role changes and the leaver feed
- Charles River and Bloomberg: key business systems with their own role models
- SharePoint: segregation of duties matrix, evidence packs and exception register

5. Process map



6. Procedure, step by step

#	Step	Who	What happens	System	Output
1	Submit the access request	Requester	Chooses the system and the role from the catalogue, states the business reason and the period needed. Temporary access must have an end date. Free-text requests for 'same as a colleague' are returned, because the colleague's access may itself be excessive. This takes 5 to 10 minutes.	ServiceNow	Access request with reason
2	Approve the business need	Line Manager	Confirms that the person needs the access for their current job. The request goes to the manager recorded in Workday and cannot be approved by the requester. Replies take 1 working day on average, and	ServiceNow	Manager approval or rejection

#	Step	Who	What happens	System	Output
			about 9% of requests are rejected here.		
3	Approve the access level	System Owner	Checks that the role matches the reason and that the level is the lowest that will do. For standard roles with low risk (about 40% of requests) the owner has pre-approved the role and this step is skipped. Privileged roles always need the owner's approval.	ServiceNow	System owner approval, or role changed
4	Check segregation of duties	Compliance Analyst	Compares the requested role with the person's existing access against the conflict matrix, for example entering trades and confirming settlements, or creating and approving payments. The check is automatic for most systems and manual for the others. About 6% of requests produce a conflict.	SailPoint IdentityIQ, SharePoint	No conflict, or conflict flagged
5	Decide on a conflict	Compliance Analyst	For a flagged conflict, either rejects the role or approves an exception with a compensating control, such as a second reviewer of all trades by the same person or a weekly report to the head of operations. Exceptions are recorded in the exception register with an expiry date of at most 12 months.	SharePoint, ServiceNow	Rejected, or exception with compensating control
6	Provision the access	Access Administrator	Assigns the group or role in Entra ID, or in the target system for the ones that are not connected, and records the ticket number against the entitlement. Connected systems provision automatically in minutes. Manual systems take up to 2 working days.	Microsoft Entra ID, target system	Access granted and recorded
7	Confirm and set the expiry	Access Administrator	Tells the requester that access is in place, sets the end date for temporary access and checks that the new entitlement appears in the next extract. About 3% of provisioned requests fail at first attempt and are retried.	ServiceNow	Request closed with audit trail
8	Launch the quarterly review	Compliance Analyst	In the first week of each quarter, extracts all entitlements from the 45 systems, checks that the extract is complete against the system's own user count and opens a campaign for each system owner and each line manager.	SailPoint IdentityIQ	Review campaigns open
9	Review every entitlement on the system	System Owner	Goes through the list of users and roles, and for each marks keep, change or remove. The review of privileged and administrator access is done in a separate list and cannot be bulk approved. A full review takes 2 to 6 hours depending on the system.	SailPoint IdentityIQ	Certified entitlement list per system
10	Review the access of direct reports	Line Manager	Reviews what each direct report can access across all systems and removes anything no longer needed. About 4% of entitlements are revoked at this review, most often access from a previous role.	SailPoint IdentityIQ	Certified entitlements per person
11	Chase and escalate late reviews	Compliance Analyst	Sends a reminder on day 5 and day 10 and, from day 15, escalates to the reviewer's director. About 20% of reviewers are late at the first deadline. A campaign is not complete until every item has a decision.	SailPoint IdentityIQ, email	All decisions recorded
12	Remove revoked access	Access Administrator	Receives a list of every item marked remove and takes it out of the system within 5	Microsoft Entra ID,	Removed access with ticket

#	Step	Who	What happens	System	Output
			working days. Records the removal against the review item so that the removal can be traced.	target system	reference
13	Send leaver and mover notices	HR Operations	Enters the leaver's last day or the mover's new role and effective date in Workday, which sends the notice to IT and to the manager. Late notices are the biggest cause of leavers keeping access. About 25% of leaver notices arrive after the last day.	Workday	Leaver or mover notice
14	Disable leaver access	Access Administrator	Disables the account at the end of the last working day, removes group memberships and removes the licence after 30 days. Applications not connected to Entra ID are removed using a checklist within 1 working day.	Microsoft Entra ID	Disabled account, checklist complete
15	Confirm access for a mover	Line Manager	Receives a list of the mover's current access, marks what is needed in the new role and what is not, and requests anything new through step 1. Access that is not confirmed within 10 working days of the move is removed automatically.	ServiceNow	Mover access confirmed or removed
16	Verify removals	Compliance Analyst	Each month compares the leaver list in Workday with active accounts in all systems and checks that every removal from the review has been done. Any account still active is raised with the administrator the same day. About 2% of leavers still have an account at 30 days.	SailPoint IdentityIQ	Verification report and exceptions
17	Build the evidence pack	Compliance Analyst	Collects the campaign results with the reviewer's name and date, the removal confirmations, the exception register and the leaver reconciliation into one pack for the quarter, stored read-only. This takes about 1 day.	SharePoint, SailPoint IdentityIQ	Quarterly evidence pack
18	Test a sample	Internal Audit	Each year picks a sample of requests, reviews and removals, checks them against the procedure and the evidence, and reports exceptions to the audit committee. Findings are tracked by compliance until closed.	SharePoint, ServiceNow	Audit report and findings

7. Decision points and business rules

- Does the line manager confirm the business need? No (about 9%): reject the request (step 2).
- Is the role pre-approved by the system owner? Yes (about 40%): skip owner approval. Privileged roles always need approval (step 3).
- Does the role conflict with the person's existing access? Yes (about 6%): reject, or approve an exception with a compensating control (steps 4 and 5).
- Is the access temporary? Yes: set an end date at provisioning (step 7).
- Did the reviewer keep, change or remove the entitlement? Remove (about 4%): administrator removes it within 5 working days (steps 9 to 12).
- Is the review late? Yes (about 20% at first deadline): remind and escalate (step 11).
- Is the person leaving? Yes: disable the account at the end of the last day (step 14).
- Has the mover's access been confirmed within 10 working days? No: remove it automatically (step 15).

- Is any leaver still active at 30 days? Yes (about 2%): raise it the same day (step 16).

8. Exceptions

- Urgent access for a deal or an incident (about 3%): the requester's director may approve by email and the administrator grants access, but the formal request must follow within 1 working day.
- Contractor without a Workday record (about 5%): the sponsor is recorded as line manager and the contract end date is the access end date.
- Shared or service account (about 2%): a named owner is recorded and reviews the account each quarter.
- System owner is also the user (about 1%): the head of the department approves instead, because nobody approves their own access.
- Leaver with a dispute or legal hold: access is disabled on the last day but data is kept for the agreed period.

9. Controls

- Nobody approves their own request or their own access review. SailPoint blocks self-approval.
- Privileged and administrator access is reviewed separately and cannot be bulk approved.
- Every entitlement carries a ticket number or a review item that shows who approved it and when.
- Segregation of duties conflicts need an exception with a compensating control and an expiry of at most 12 months.
- Review campaigns use a complete extract, checked against the system's own user count before they open.
- A leaver reconciliation against Workday runs monthly, and any account still active after 30 days is reported to the head of IT.
- Evidence packs are stored read-only for 7 years.

10. Known issues today

- Requesters ask for 'same as a colleague' and old excess access is copied from person to person.
- Reviewers click approve on the whole list without reading it, especially for large systems.
- Manual systems that are not connected to the identity platform are provisioned late, and removals there are forgotten.
- HR notices arrive after the leaver's last day, so accounts stay active.
- Roles in business systems are not named in a way a manager understands, so reviews rely on the administrator's explanation.
- Evidence is collected by hand at the end of the quarter, so audit requests take days.

11. RACI matrix

R = responsible (does the work), A = accountable (owns the outcome), C = consulted, I = informed.

Activity	Requester	Line Manager	System Owner	Access Admin	Compliance	HR Operations	Internal Audit
Submit the request	A/R	I					
Approve the business need	I	A/R					
Approve the access level	I	C	A/R	I			
Check segregation of duties		I	C		A/R		
Provision the access	I		C	A/R			
Run the quarterly review		R	R	I	A		I
Remove revoked access	I	I	C	A/R	I		

Activity	Requester	Line Manager	System Owner	Access Admin	Compliance	HR Operations	Internal Audit
Notify leavers and movers		C		I	I	A/R	
Disable leaver access		I		A/R	I	C	
Keep evidence and test it				C	A/R		R

12. KPIs

KPI	Definition	Target
Requests provisioned within target	Share of approved requests provisioned within 2 working days of the last approval.	[set]
Review completion by the deadline	Share of review campaigns fully decided by the end of day 15. Today about 80%.	[set]
Entitlements revoked at review	Share of reviewed entitlements marked remove. Today about 4%. A rate near zero suggests reviewers are not reading the list.	[set]
Leavers with active access after 30 days	Number of leavers who still have an active account in any system 30 days after the last day. The target is zero.	[set]
Open segregation of duties exceptions	Number of approved exceptions, and how many are past their expiry date.	[set]
Audit findings open	Number of findings from internal audit on access that are still open, with age.	[set]

13. Revision history

Version	Date	Author	Change
1.0	[date]	[name]	First as-is version

Free template from processfix.ai. You may copy and adapt it. The company in the example is fictional.