

Physical key control policy template

This template provides operating rules for a team handling physical keys. It is not effective until your organization has completed the customization fields, selected its handover rule and approved the finished document.

Instructions before adoption

Replace every [CUSTOMIZE] field. Choose either handover option A or B and remove the other. Confirm the procedures fit your property authority, client instructions and applicable requirements. Check that the named contacts can actually receive reports. Remove these instructions and the template attribution when issuing your approved policy.

Organization: [CUSTOMIZE]

Policy owner and deputy: [CUSTOMIZE]

Approved by: [CUSTOMIZE]

Version and approval date: [CUSTOMIZE]

Effective date and next review date: [CUSTOMIZE]

Sites and key categories covered: [CUSTOMIZE]

Related access or electronic credential procedures: [CUSTOMIZE]

1 Purpose and scope

This policy establishes how the organization authorizes, issues, records, safeguards and recovers the physical keys within its stated scope. It applies to employees and other people issued those keys, including approved contractors and temporary workers.

A custody record documents the reported movement or possession of a key set. It does not itself authorize entry to premises. Recipients must observe the approved purpose, site restrictions and access conditions for their assignment.

2 Responsibilities and contacts

The policy owner approves the operating process, assigns deputies, arranges reviews and resolves matters outside routine authority. The authorizer confirms whether a recipient may receive the specified keys for the stated purpose. The custodian maintains the inventory and movement records and coordinates checks and follow-up.

Each holder safeguards the keys, uses them only for the authorized purpose, follows the selected handover rule and reports discrepancies. A receiver checks the set before confirming its return. One person may perform more than one role where approved by the policy owner.

Routine authorizer and deputy: [CUSTOMIZE]

Custodian and deputy: [CUSTOMIZE]

Incident decision-maker and deputy: [CUSTOMIZE]

Incident reporting channel during office hours: [CUSTOMIZE]

Out-of-hours channel and fallback if unanswered: [CUSTOMIZE]

3 Authorization before issue

Keys may be issued only to an identified individual with approval for the specified set and purpose. Before release, the issuer must verify the recipient against the approval and check relevant access limits. A company name alone is not an adequate holder record.

Approval must be recorded in [CUSTOMIZE system or location], including the approver, recipient, purpose, scope and any time restrictions. Exceptions require approval by [CUSTOMIZE role]. Approval to use the record system must not be treated as authorization to enter a property.

4 Inventory and storage

The custodian must maintain a register of the key sets in scope, their unique references, expected contents, authorized property mapping, storage positions and recorded status. Distinguishable copies or sets must not share an ambiguous reference. Record authorized additions, removals and replacements.

Physical tags must use the approved reference format [CUSTOMIZE]. Property addresses, alarm codes and access instructions must not be placed on tags under this policy. Access to the property mapping and records is limited to [CUSTOMIZE roles].

Keys not issued must be kept in [CUSTOMIZE approved secure storage]. Storage access is restricted to [CUSTOMIZE roles]. Unknown or duplicate-labeled sets must receive a temporary reference and an entry recording their markings, discovery location and any temporary move. Permanent identification or relabeling requires the custodian's authorized review.

5 Issue and acknowledgement

Before release, the issuer and recipient must check the set reference and contents. Record the recipient, issuer, purpose or job reference, approval reference, actual issue time, return deadline and agreed return destination. Receipt must be acknowledged by [CUSTOMIZE approved method].

All movement records use [CUSTOMIZE timezone and date format]. For ongoing assignments, record the review date and recall conditions in [CUSTOMIZE location]. The issuer must explain relevant storage, transfer, return and incident instructions to the recipient.

If the normal record system is unavailable, use [CUSTOMIZE approved fallback record]. The custodian must reconcile fallback entries into the main record by [CUSTOMIZE deadline]. Preserve the actual event time and separately identify the time of later entry. Do not invent an event time where it is unknown.

6 Handover rule

CUSTOMIZATION REQUIRED Select option A or option B and delete the other before approval. Do not adopt both.

Option A Return to storage before reissue

Direct transfers between holders are prohibited. The holder must return the set to an approved receiver, who checks and records receipt. A fresh issue may then be made to an authorized recipient. A request from a colleague or contractor does not override this rule. Exceptional arrangements require prior approval by [CUSTOMIZE role] and a documented custody procedure.

Option B Approved direct handovers

Direct transfers are permitted only after authorization has been checked for the named recipient and the particular assignment. Before passing the set, both people must check its reference and contents and confirm the return

destination and deadline. At receipt, record the transfer time and recipient's acknowledgement in [CUSTOMIZE record].

A pending request or message does not establish a completed transfer. If the recipient declines or does not acknowledge receipt, the sender must retain the set and contact the custodian. If physical transfer has already occurred without the required record, report the discrepancy promptly, establish the actual circumstances and add a correction with its source. Do not fabricate a return to storage or an acknowledgement.

Under option B, the existing deadline remains unless [CUSTOMIZE role] approves a change. Record both deadlines, the approver and approval time. A transfer does not extend access permission beyond the authorized purpose or period.

7 Copies and higher-access keys

No holder may copy a key or arrange a lock change without approval from [CUSTOMIZE role]. Approved copies must be made through [CUSTOMIZE authorized provider or process] and entered into the inventory before issue. Record the reason, approval and resulting copy or set reference.

The following sets require additional controls: [CUSTOMIZE master keys or other higher-access sets]. Their approval authority, storage conditions, issue limits and review arrangements are [CUSTOMIZE]. A request for a replacement must also address the status of the original key.

8 Return and changes of assignment

Keys must be returned by the agreed deadline, when recalled by an authorized person, or when no longer required for the approved assignment. The receiver must check the reference and contents, record the actual receipt time and receiver, and confirm the storage position before marking the set fully returned and available.

A deposit at an approved collection point [CUSTOMIZE location or state not permitted] is a reported return until checked by an authorized receiver. Keep the deposit report separate from confirmed receipt. Do not record an unverified receipt as fact.

For a partial return, record which keys were received and which remain unaccounted for. Preserve the discrepancy and follow the incident procedure as appropriate; do not close the whole set as completely returned.

On departure, role change or contract completion, [CUSTOMIZE responsible role] must review issued keys, arrange recovery and document unresolved items. Removing system access does not recover physical keys and must be handled as a separate task.

9 Overdue records and incidents

The custodian or deputy must review open checkouts at [CUSTOMIZE frequency] and follow up overdue entries with the recorded holder. An authorized extension must preserve the original deadline and identify the new deadline, approver and time of approval.

Anyone discovering or suspecting loss, theft, unauthorized transfer, unauthorized use or an unexplained missing key must notify the incident contact without delay. If the primary route is unanswered, use the stated fallback. Follow the organization's emergency procedure where immediate danger is involved.

Record the key reference, known facts, last confirmed event, reporting time, reporter and actions taken. Distinguish confirmed facts from reported information or assumptions. Do not wait for a scheduled audit or follow-up date to raise an urgent concern.

The incident decision-maker must assess the access at risk, required notifications and protective action, including whether authorized lock changes are needed. Record decisions, owners and review deadlines. Finding a missing key

does not automatically close the incident; the decision-maker must review any continuing concern and record closure.

10 Reconciliation and follow-up

The custodian must arrange inventory reconciliation at [CUSTOMIZE frequency], and after [CUSTOMIZE events or changes]. Check registered sets against storage and holder confirmations, and check sets found in storage against the register.

For each discrepancy, record the reference, observation, confirmation method, action owner and follow-up date. Distinguish reported possession from a physical check. Carry temporary references for unknown or duplicate-labeled sets through every related record until authorized identification is complete.

The reviewer [CUSTOMIZE role] must record the outcome, unresolved items and next actions. A follow-up deadline is a review date, not permission to delay urgent incident reporting. Corrections must explain what was established, by whom and when.

11 Records and information handling

Keep the inventory, movement records, approvals, acknowledgements, incident records and review outcomes in [CUSTOMIZE approved locations]. Access is restricted to [CUSTOMIZE roles and purposes]. Do not add access codes or unnecessary personal information to movement logs or printed tags.

Paper corrections must leave the original readable and identify the person and date of correction. Electronic corrections must preserve the original event and explain the correction through a change history or linked amendment. An ordinary user must not silently erase an earlier movement to make a record appear complete.

The policy owner must approve retention periods for each record type in [CUSTOMIZE retention schedule]. Records required for an unresolved incident or other applicable preservation requirement must not be disposed of until authorized. Disposal at the end of the approved period must follow [CUSTOMIZE secure disposal procedure].

12 Exceptions and policy review

Departures from this policy require approval by [CUSTOMIZE role], a recorded reason, the affected keys and people, any additional controls and an expiry or review date. Recording an exception does not authorize access beyond the organization's authority or the applicable site conditions.

The policy owner must review this policy on its stated review date and after relevant process changes or incidents. Record the version, approver, effective date and reason for substantive changes. Staff and other recipients must receive the instructions relevant to their role before being issued keys.

Approval and issue record

Approved policy version: [CUSTOMIZE]

Approver name and role: [CUSTOMIZE]

Approval acknowledgement and date: [CUSTOMIZE]

Location of the approved copy: [CUSTOMIZE]

How affected people will be informed: [CUSTOMIZE]

Original operational template prepared by KeyDocket. Adapt before adoption. This template does not certify compliance, create a liability agreement or set financial penalties.