[Company name]

Employee Offboarding Checklist

Owner	[People owner role]
Applies to	Every employee and contractor who held access to company systems
Version	[Version]

1. Departure

Person leaving:

Role:

Employee or contractor:

Effective termination date and time:

Voluntary or involuntary:

Manager:

Checklist run by:

2. Block one: the clock

No.	Step	Owner	Evidence it has to produce	Done on
1	Fix the effective termination date and time in writing	Human resources	Personnel record carrying the effective date	
2	Disable the identity provider account and revoke every live session and refresh token	IT owner	Directory log line with the timestamp, plus the session revocation record	
3	Rotate any shared secret the person could still use from memory	Security lead	Rotation record naming the secret, dated	
4	Remove production console and cloud access, including local accounts that never federated	Engineering lead	Exported change event from the cloud provider	
5	Remove source control, pipeline and deploy rights, and revoke tokens and deploy keys	Engineering lead	Audit log showing each removal with its timestamp	
6	Reassign what the person owned: on call, alert routing, named controls	Their manager	Updated rotation and ownership records, dated	

3. Block two: the systems outside your identity provider

No.	Step	Owner	Evidence it has to produce	Done on
7	Delete cloud access keys and command line credentials	Engineering lead	Key deletion event from the provider audit trail	
8	Remove secure shell keys, bastion entries and virtual private network certificates	Engineering lead	The removed key fingerprint, with the commit or log line	
9	Drop database and warehouse logins that were created by hand	Data owner	Console record or the executed statement, dated	
10	Deprovision software bought on a card and never wired to single sign on	Finance and IT	Vendor register with a removal date beside each tool	
11	Remove vault entries, shared mailboxes and guest access in external channels	IT owner	Membership export taken after removal	
12	Remove customer facing access: support desk, admin panels, partner portals	Support lead	Removal record naming the tool and the date	

4. Block three: hardware and physical access

No.	Step	Owner	Evidence it has to produce	Done on
13	Recover the laptop, phone and hardware security key	IT owner	Asset register row with the serial number and return date	
14	Deactivate the building badge and collect any physical key	Office manager	Badge system record showing the deactivation date	
15	Wipe or reimage before reissue, or log the remote wipe if it never comes back	IT owner	Wipe confirmation carrying the serial number and date	

5. Block four: the record

No.	Step	Owner	Evidence it has to produce	Done on
16	Complete the checklist, name the person, date it, and have one person sign it	Human resources	The completed checklist itself, signed and dated	
17	Reconcile your offboarding records against the human resources leaver list	Human resources	The two lists side by side, with counts and differences explained	
18	File every artifact so it can be pulled a year later by date	Compliance owner	Stored evidence set, indexed by name and date	

6. Sign-off

Every step above has a date and the evidence it produced is filed. Any step not done is explained in writing below.

Exceptions and explanations:

Checklist completed by

Name:

Signature:

Date:

Reviewed by

Name:

Signature:

Date:

7. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Version]	Start at 1.0 and increase it each time the document changes.
[People owner role]	The role that runs hiring and departures, for example head of people.

Source

Source: free template from cybersoftware.com/templates/offboarding-checklist (CC BY 4.0).