

DATA LOSS PREVENTION SERIES

How to Keep Data Safe When Offboarding Employees

A practical, step by step framework for IT, HR, and security leaders to protect sensitive data before, during, and after an employee departs.

Know the risks. Follow the process. Use the checklist.

INSIDE THIS GUIDE

How to use this guide

Read it end to end to build your offboarding program, or jump straight to the checklist in Part 6 and use it as a working tool for your next departure.

CONTENTS

Part	What it covers
Introduction	The most overlooked moment in data security.
Part 1: How data leaves	Common exit routes, the three types of departing employee risk, and the cost of getting it wrong.
Part 2: Build a secure foundation	Data classification, access inventory, least privilege, device and web controls, policies, HR and IT alignment.
Part 3: When notice is given	Risk assessment, activity review, increased visibility, gradual access reduction, documentation.
Part 4: The last day	Disable accounts, rotate credentials, recover devices and data, security focused exit interview.
Part 5: After departure	Verify and improve.
Part 6: The checklist	A ready to use offboarding data security checklist.
Part 7: How CurrentWare helps	Offboarding challenges mapped to controls.

WHAT YOU WILL LEARN

- The most common ways data leaves with departing employees.
- What to put in place now so every offboarding starts from a secure baseline.
- How to identify and respond to risky behavior during the notice period.
- A complete last day access revocation process, plus a ready to use checklist.

THE PRINCIPLES, WHATEVER YOUR SIZE

Whether you manage offboarding for a 50 person business or a 5,000 person enterprise, the principles are the same. Know your data: understand what sensitive information you hold and where it lives. Know who can reach it: keep a clear record of every account, system, and device each employee uses. Close every door on time: watch for warning signs and remove access exactly when employment ends.

The most overlooked moment in data security

Every employee who leaves your company walks out the door with knowledge, relationships, and habits. Too often, they also walk out with your data. Offboarding is one of the highest risk moments in the employee lifecycle. The departing employee still has legitimate access to systems, files, and customer records. They may be heading to a competitor. They may feel entitled to "their" work. Or they may simply be careless in their final days, forwarding files to a personal inbox so they have samples for their portfolio. Most organizations invest heavily in keeping outsiders out. Far fewer have a structured process for what happens when a trusted insider becomes a former employee. That gap is where client lists, source code, pricing models, and confidential documents quietly disappear.

How data leaves with departing employees

Before you can stop data exfiltration, you need to know what it looks like. Departing employee data loss usually falls into three categories: malicious theft, well intentioned but careless copying, and lingering access that nobody remembered to remove.

Exit route	What it looks like	Why it is hard to spot
USB and external drives	Copying folders to a flash drive or external hard drive in the final weeks	Happens offline, often leaves no trace in cloud or email logs
Personal cloud storage	Uploading files to personal Google Drive, Dropbox, OneDrive, or WeTransfer	Traffic looks like normal web browsing
Personal email	Forwarding attachments or entire threads to a personal address	Blends in with routine email activity
Printing and screenshots	Printing customer lists or capturing screens with a phone	Physical and offline, bypasses most digital controls
SaaS and shadow IT accounts	Keeping access to CRM, project tools, or apps signed up for with a work email	IT may not know the account exists
Lingering credentials	Shared passwords, VPN access, or API keys that are never rotated	Access remains valid long after the last day
Company devices	Laptops or phones returned late, wiped by the employee, or never returned	Data on the device leaves with it

How data leaves with departing employees

The three types of departing employee risk

Type	What it means
The malicious insider	A small share of departing employees deliberately take data to gain an edge at a new employer, start a competing business, or retaliate. They often act in the weeks before giving notice, so detection has to start before the resignation letter.
The negligent insider	Far more common is the employee who believes their work belongs to them. They copy presentations, templates, and contact lists "for reference" without realizing they are breaching policy, contracts, or privacy law.
The forgotten account	Sometimes the employee does nothing wrong at all. The risk comes from access that stays open: an active login, a synced mobile device, or a shared admin password that attackers can later exploit.

The cost of getting it wrong

The consequences of offboarding data loss go well beyond the value of the files themselves. Organizations face lost competitive advantage, breach notification obligations, regulatory penalties under frameworks like GDPR, HIPAA, and PCI DSS, costly litigation to recover trade secrets, and damaged client trust.

A single lost customer list can undo years of sales effort

The files are rarely the expensive part. The notification obligations, the litigation, and the client conversations are.

Build a secure foundation before anyone resigns

Secure offboarding starts on an employee's first day, not their last. The organizations that handle departures smoothly are the ones that already know what data exists, who can access it, and what normal behavior looks like.

What to put in place	
1 Classify your sensitive data	You cannot protect what you have not identified. Map where your most valuable data lives, such as customer databases, financial records, intellectual property, HR files, and source code. Label it by sensitivity so you know which departures need the closest attention.
2 Keep a living access inventory	For every employee, maintain a record of the systems, applications, shared drives, devices, and credentials they hold. Update it whenever someone changes roles. When a departure happens, this inventory becomes your revocation checklist instead of a guessing game.
3 Enforce least privilege	Give employees only the access their role requires. Review permissions quarterly and remove anything that has built up through role changes and one off projects. The less access a person has, the less they can take with them.
4 Control removable media and file transfers	USB drives remain one of the simplest ways to move large volumes of data without detection. Set a clear policy on which devices are allowed, block unauthorized storage devices, and log file transfers to approved ones. This way a departing employee cannot quietly copy a shared drive onto a thumb drive.
5 Restrict risky websites and cloud uploads	Block or limit access to personal cloud storage, file sharing services, and personal webmail on company devices, or allow them only for teams with a business need. Web filtering closes some of the most common exfiltration routes.
6 Establish a baseline of normal activity	Monitoring tools are most useful when you know what normal looks like. Tracking web and application usage over time lets you spot unusual spikes, such as a sudden surge in cloud storage visits or late night file activity.
7 Put it in writing	Make sure employment contracts, acceptable use policies, and confidentiality agreements clearly state that company data belongs to the company. Be transparent that company devices are monitored for security purposes. Clear, communicated policies deter negligent behavior and strengthen your legal position if you need to act.
8 Align HR and IT	Many offboarding failures happen because IT learns about a departure too late. Create a formal trigger so HR notifies IT and security the moment a resignation or termination is confirmed, ideally through a shared ticket or workflow.

When notice is given, assess and monitor

The notice period is when risk peaks. The employee still has full access, their loyalty may already be shifting, and colleagues may be distracted by handover work. Treat this window as an active security phase.

1. Assess the risk level of the departure

Not every departure carries the same risk. Score each one against a few simple questions:

- ☐ Does the employee have access to highly sensitive data, such as customer lists, IP, or financials?
- ☐ Are they joining a competitor or starting a similar business?
- ☐ Is the departure voluntary, or is it a termination or layoff?
- ☐ Do they hold admin or privileged accounts?
- ☐ Have there been any recent performance, conduct, or morale concerns?

High risk departures, such as an involuntary termination of a privileged user, may call for immediate access removal rather than a standard notice period.

2. Review recent activity

Many insiders begin collecting data before they resign. Review the last 30 to 90 days of activity for signs like these:

- ☐ Large or unusual file transfers to USB or external drives
- ☐ Frequent visits to personal cloud storage or file sharing sites
- ☐ Bulk downloads from the CRM, document management system, or shared drives
- ☐ Emails with attachments sent to personal addresses
- ☐ Access to files or systems outside their normal role
- ☐ Activity at unusual hours or on weekends

When notice is given, assess and monitor

3. Increase visibility for the remaining period

For the rest of the notice period, keep a closer watch on the employee's computer activity in line with your written policies. Set real time alerts for high risk actions, such as connecting an unapproved storage device or visiting blocked file sharing sites. Consider tightening controls further, for example by setting USB access to read only or blocking uploads to cloud storage for that user.

4. Start reducing access gradually

As the employee hands over responsibilities, remove access they no longer need. Transfer ownership of shared files, projects, and client accounts to their replacement or manager. Gradual reduction lowers risk without disrupting the handover.

5. Document everything

Keep a record of what was reviewed, what alerts fired, and what actions were taken. If an incident occurs, this documentation supports investigations, legal action, and compliance reporting.

A note on privacy and trust

Monitoring should always be proportionate, transparent, and consistent with local laws and your own policies. Apply the same process to every departing employee in a given risk tier so that no one feels singled out.

The last day, close every door

The final day is about precision and timing. Access should end at the agreed moment: not days later, and not so early that the handover suffers. Use your access inventory to work through each area in turn.

Order	Step
1	HR confirms exit time
2	Disable accounts and sessions
3	Rotate shared credentials
4	Recover devices and assets
5	Exit interview and reminders
6	Confirm and document

This sequence keeps access removal tightly coordinated with the employee's departure time.

Disable accounts and sessions

- ☐ Disable the network and directory account (for example, Active Directory or Microsoft Entra ID)
- ☐ Revoke email access and set up forwarding or an auto reply as needed
- ☐ Remove VPN, remote desktop, and Wi-Fi access
- ☐ Terminate active sessions and sign out of all devices
- ☐ Remove access to SaaS apps, including CRM, ERP, collaboration, and project tools
- ☐ Revoke multi factor authentication tokens and registered devices
- ☐ Deactivate building access cards and physical keys

Tip

For planned departures, schedule account suspension in advance so access ends automatically at the exact exit time, even if the process owner is unavailable.

The last day, close every door

Rotate shared credentials

Any password the employee knew should be treated as compromised. Change shared account passwords, admin credentials, Wi-Fi keys, and alarm codes. Rotate API keys, service account credentials, and SSH keys they had access to. A password manager with shared vaults makes this far easier.

Recover company devices and data

- ☐ Collect laptops, phones, tablets, external drives, and security tokens
- ☐ Check devices against your asset register
- ☐ Preserve device data before wiping, especially for high risk departures where an investigation may follow
- ☐ Remotely wipe company data from personal devices enrolled in BYOD programs
- ☐ Confirm that company files have been removed from personal storage, and get written confirmation where possible

Hold a security focused exit interview

Use the exit interview to remind the employee of their continuing confidentiality and non disclosure obligations. Ask them to confirm in writing that they have returned all company property and data. Ask about accounts IT may not know about, such as tools they signed up for with their work email.

After departure, verify and improve

Offboarding does not end when the employee leaves the building. The weeks that follow are your chance to confirm nothing was missed.

	What to do
1 Audit for lingering access	About 30 days after departure, run an access review. Look for accounts still active, login attempts from the former employee's credentials, and apps that were missed in the original sweep. Former employee accounts that stay active are a favorite target for attackers.
2 Review activity logs	Check device, file, and web activity reports from the final weeks of employment. If you find evidence of data exfiltration, act quickly: involve legal counsel, preserve evidence, and follow your incident response plan.
3 Manage retained data	Decide how long to keep the former employee's mailbox, files, and device images based on legal, regulatory, and business requirements. Archive what you must keep and securely delete the rest.
4 Learn from every departure	After each offboarding, ask what worked and what did not. Did IT get notice in time? Were any accounts missed? Use the answers to refine your checklist and your tools.

Offboarding is a cycle, not a single event

Every lesson from a departure should feed back into the foundations in Part 2. Over time, each offboarding becomes faster, more consistent, and more secure.

The offboarding data security checklist

Use this checklist for every departure. Print it, add it to your ticketing system, or adapt it to your own workflow.

Before any departure (ongoing)

- ☐ Sensitive data is classified and mapped
- ☐ Each employee's access is recorded in a current inventory
- ☐ Permissions follow least privilege and are reviewed quarterly
- ☐ USB and removable media are controlled and logged
- ☐ Personal cloud storage and file sharing sites are restricted
- ☐ Baseline activity monitoring is in place
- ☐ Confidentiality, acceptable use, and monitoring policies are signed
- ☐ HR has a formal trigger to alert IT of departures

When notice is given

- ☐ Departure risk level assessed
- ☐ Last 30 to 90 days of activity reviewed
- ☐ Real time alerts set for high risk actions
- ☐ Additional restrictions applied where appropriate
- ☐ File, project, and client ownership transferred
- ☐ Unneeded access removed as handover progresses
- ☐ Actions and findings documented

The offboarding data security checklist

On the last day

- ☐ Directory, email, VPN, and remote access disabled
- ☐ Active sessions terminated on all devices
- ☐ SaaS and third party app access removed
- ☐ MFA tokens and registered devices revoked
- ☐ Shared passwords, API keys, and service credentials rotated
- ☐ Laptops, phones, drives, and tokens collected
- ☐ Device data preserved before wiping, if needed
- ☐ Company data wiped from BYOD devices
- ☐ Building access cards and keys deactivated
- ☐ Exit interview completed and confidentiality reminder signed

After departure

- ☐ 30 day access audit completed
- ☐ Final weeks' activity logs reviewed
- ☐ Retained data archived or securely deleted
- ☐ Process reviewed and checklist updated

How CurrentWare helps you offboard securely

A checklist is only as strong as the tools that enforce it. CurrentWare gives IT and security teams the visibility and control to protect data at every stage of offboarding, from a single, easy to deploy console.

Offboarding challenge	CurrentWare solution	How it helps
Data copied to USB drives	AccessPatrol	Block unauthorized USB and peripheral devices, set read only access, and log file transfers to approved storage devices
Uploads to personal cloud storage and file sharing sites	BrowseControl	Block websites by category, including cloud storage and file sharing, and restrict unapproved applications
Spotting warning signs during the notice period	BrowseReporter	Track web and application usage, compare activity against normal patterns, and review what employees did in their final weeks
Access that stays open after the last day	enforceIT	Schedule automatic computer and user account suspension so access ends exactly when it should
Proving what happened	The CurrentWare Suite	Detailed reports and alerts create an audit trail to support investigations and compliance

Why IT teams choose CurrentWare

	What it means
Built for data loss prevention	Control the most common exfiltration routes, including removable media, websites, and applications.
Proactive alerts	Get notified in real time when a user attempts a risky action, so you can respond before data leaves.
Works on and off the network	Policies stay enforced for remote and hybrid employees.
Flexible deployment	Run it on premises or in the cloud to suit your environment.
Modular and scalable	Start with the solution you need most and add more as your program grows.

Turn your offboarding checklist into automated protection

Every departing employee is a potential data leak. With CurrentWare, you can see risky behavior early, block the easiest ways out, and make sure access ends right on time.

Start your free trial: currentware.com/download • Book a demo: currentware.com/demo

MORE RESOURCES

What to read alongside this

The templates and checklists that support each part of this guide.

Resource	URL
Employee Offboarding Checklist (the per-departure record)	https://www.currentware.com/blog/how-to-keep-data-safe-when-offboarding-employees/
Removable Media Policy Template (Part 2)	https://www.currentware.com/blog/removable-media-policy-template/
Workplace Monitoring Policy Template (Part 3)	https://www.currentware.com/blog/workplace-monitoring-policy-template/
Employee Monitoring Compliance Checklist	https://www.currentware.com/blog/employee-monitoring-laws/
Get a Free Trial of CurrentWare	https://www.currentware.com/download/

ABOUT

About CurrentWare

CurrentWare provides employee monitoring, web filtering, device control, and data loss prevention software that helps organizations protect sensitive data and improve productivity.

CurrentWare's solutions are adopted by a wide array of government and private organizations including schools, hospitals, libraries, and for-profit businesses.

ONE PLATFORM. FOUR MODULES.



Device control and data loss prevention: block unauthorized USB devices, set read only access, and log file transfers. Part 2 and Part 4.



Web and application filtering: block cloud storage and file sharing categories at the point of collection. Part 2.



Activity monitoring and alerting: baseline normal behavior and review the final weeks. Part 3 and Part 5.



Remote power management and logon reporting across endpoints.

See risky behavior early, and close every door on time

Block the easiest ways out, get alerted before data leaves, and keep the audit trail that supports an investigation if one follows. On premises or in the cloud.

Start a 14-day free trial: currentware.com/download • Book a demo: currentware.com/demo

Disclaimer

Not legal advice

This guide is provided for general informational purposes only and does not constitute legal advice. Consult qualified legal counsel about employee monitoring and data protection requirements in your jurisdiction.

Part 3 describes increasing monitoring of a named individual during their notice period. In several jurisdictions that carries its own notice, proportionality and retention obligations, and in some it requires consultation before it begins. Confirm your position before treating a departure as a heightened-monitoring case.

CurrentWare makes no representation or warranty as to the accuracy or completeness of this information and accepts no liability for any action taken in reliance on it.

ABOUT THIS DOCUMENT

This edition restyles the guide to the current CurrentWare house standard, makes the Part 6 checklist and the assessment lists fillable, and cross-links each part to the companion template that supports it. The guidance itself is carried over unchanged from the previous version.