

# How to Use This Template

This employee offboarding checklist template is provided by CurrentWare Inc. for use and adaptation by your organization. You may need to modify the contents of this template to meet the unique needs of your environment.

This template can be printed as a standard document or used digitally as an interactive form with fields for text, digital signatures, and checkboxes. For the best experience you should use [Adobe Acrobat Reader](#) or the latest version of Microsoft Edge as your PDF viewer.

**Offboarding Checklist To Preserve Data Security**

**Employee Information**

Employee Name: \_\_\_\_\_ Employee ID: \_\_\_\_\_

Resignation Date: \_\_\_\_\_

Last Day of Work: \_\_\_\_\_

**Communication**

✓	Item	Date	Staff Member	Comments
<input type="checkbox"/>	Removed mentions from internal documentation (contacts lists, org charts, websites, etc)		<input type="checkbox"/>	
<input type="checkbox"/>	Statements signed confirming that all company-owned assets have been returned and access to systems has been revoked		<input type="checkbox"/>	
<input type="checkbox"/>	Departure announced to relevant parties including IT personnel, clients, and vendors that the employee worked with		<input type="checkbox"/>	
<input type="checkbox"/>	Exit interview performed All policies have been reacknowledged		<input type="checkbox"/>	
<input type="checkbox"/>			<input type="checkbox"/>	
<input type="checkbox"/>			<input type="checkbox"/>	

DIGITAL SIGNATURE FIELD  
(ACROBAT DESKTOP APP ONLY)

TEXT FIELD

CLICKABLE CHECKBOX

**Disclaimer:** The contents of this template are provided by CurrentWare Inc. for informational purposes only. The information shared in this template does not constitute legal advice or security consultation from CurrentWare. Designated specialists must be consulted prior to the implementation of any policy, technology, or related resource in your organization.

# Offboarding Checklist To Preserve Data Security

## Employee Information

Employee Name: \_\_\_\_\_ Employee ID: \_\_\_\_\_

Resignation Date: \_\_\_\_\_

Last Day of Work: \_\_\_\_\_

## Communication

✓	Item	Date	Staff Member	Comments
	Removed mentions from internal documentation (contacts lists, org charts, websites, etc)			
	Statements signed confirming that all company-owned assets have been returned and access to systems has been revoked			
	Departure announced to relevant parties including IT personnel, clients, and vendors that the employee worked with			
	Exit interview performed: All policies have been reacknowledged			

# Offboarding Checklist To Preserve Data Security

## Account and Access Deprovisioning

✓	Item	Date	Staff Member	Comments
	Provided designated individual(s) with access to the ex-employee's files			
	Revoked access to corporate assets such as social media accounts, domain logins, remote access tools, and IAM			
	Passwords changed on shared accounts that the employee had access to			
	Email access revoked, with emails forwarded to a designated replacement			
	Ownership of systems previously controlled by the ex-employee have been transferred			
	Telephone is not forwarded to any external numbers that the ex-employee can access			
	Voicemail accounts have been deprovisioned			
	Physical access control devices such as door codes and/or locks have been changed			

# Offboarding Checklist To Preserve Data Security

## IT Inventory Control

✓	Item	Date	Staff Member	Comments
	Company assets have been returned including computers, mobile devices, external storage devices, and access cards			
	Backups of critical files have been created and validated			
	Corporate data stored on the ex-employee's personal devices has been backed up and wiped from their devices			
	All materials related to projects the ex-employee was working on have been returned			
	Files that have been stored outside of primary repositories have been moved to a designated secure location			

# Offboarding Checklist To Preserve Data Security

## Digital Forensics, Compliance, & Auditing

✓	Item	Date	Staff Member	Comments
	A forensic image of the employee's computer has been created and logged for retention			
	An individual has been designated to monitor the network for suspicious activity			
	Alerts for anomalous or high-risk computer usage have been created			
	Network printer activity has been reviewed for high-risk anomalies			
	Email usage is being monitored for high-risk communications and/or file activity			

# Offboarding Checklist To Preserve Data Security

## Other Items

✓	Item	Date	Staff Member	Comments

# Offboarding Checklist To Preserve Data Security

## Other Items

✓	Item	Date	Staff Member	Comments

# More Resources





Resource	URL
Internet Usage Policy Template	<a href="https://www.currentware.com/internet-usage-policy-template/">https://www.currentware.com/internet-usage-policy-template/</a>
Work From Home Policy Template	<a href="https://www.currentware.com/work-from-home-policy-template/">https://www.currentware.com/work-from-home-policy-template/</a>
Removable Media Policy Template	<a href="https://www.currentware.com/blog/removable-media-policy-template/">https://www.currentware.com/blog/removable-media-policy-template/</a>
How to Keep Data Safe When Offboarding Employees	<a href="https://currentware.com/how-to-keep-data-safe-when-offboarding-employees/">https://currentware.com/how-to-keep-data-safe-when-offboarding-employees/</a>
The CurrentWare Blog	<a href="https://www.currentware.com/blog/">https://www.currentware.com/blog/</a>
Get a Free Trial of CurrentWare	<a href="https://www.currentware.com/download/">https://www.currentware.com/download/</a>

## About CurrentWare

CurrentWare is a software company that provides a suite of workforce management solutions for computer monitoring, content filtering, data loss prevention, and remote power management.

CurrentWare's solutions are adopted by a wide array of government and private organizations including schools, hospitals, libraries, and for-profit businesses. CurrentWare customers improve their user productivity, data security, and business intelligence with advanced awareness and control over how technology is used in their organization.

For more information you can visit our website at [www.CurrentWare.com](http://www.CurrentWare.com)

 AccessPatrol	Data loss prevention software to restrict and monitor USB device activity.
 BrowseControl	Content filtering software to restrict internet access and block the use of applications.
 BrowseReporter	Employee monitoring software that tracks website and application usage.
 enPowerManager	Remote device management software for configuring computer settings such as power states.