



The Employee Offboarding Checklist

12 steps to close the data door behind every leaver.

One forwarded customer file is all it takes. This checklist is what we use at Sirius Star sites — adapted for industrial SMB operations, before formal IT systems exist. Use it for every resignation, termination, contract end, and seasonal-staff exit. No exceptions.

Section 1: Day of Notice

- | | | | |
|----|--|----|--|
| 01 | Document handover plan agreed and signed | 02 | Email auto-forward set up to manager (with email log retained) |
| 03 | Customer-facing accounts: ownership transferred (CRM, support inbox) | 04 | Accounts/payroll informed of last working day |

Section 2: Last Working Day

- | | | | | | |
|----|--|----|--|----|---|
| 01 | Email + Microsoft 365 / Google Workspace access disabled at 6 PM | 02 | Tally / ERP user disabled, not deleted (audit trail preserved) | 03 | VPN / remote-access credentials revoked |
| 04 | Personal devices wiped of company data (signed declaration) | 05 | Physical access cards / keys returned, log signed by admin | | |

Section 3: Within 24 Hours

- | | | | | | |
|----|---|----|---|----|---|
| 01 | Manager review: "What did this person have access to that we missed?" | 02 | Customer-master and design files: timestamp + integrity check | 03 | Exit interview: 3 questions about systems, gaps, what we should fix |
|----|---|----|---|----|---|

✔ This checklist plus the data map (Field Guide Vol 1) are your two highest-leverage data-safety artefacts. Together they catch 85 per cent of the leaks we see in the wild.