13-Steps to Mitigate Risks
of Employee BYOD Cell Phone Usage

When employees using their mobile devices for business purposes leave the company, their departure creates risks of data leakage, IP loss, and reputational damage.

Address and mitigate these risks by taking these 13 steps.

PROACTIVE STEPS

- ❑ Implement and install Mobile Device Management (MDM) on all employee-owned devices.
- ❑ Require employees to use two-factor authentication (2FA) to access company data on their personal devices.
- ❑ Enforce encryption of all company data.
- ❑ Create and enforce an Acceptable Use Policy.
- ❑ Create a Bring Your Own Device (BYOD) policy that gives the company rights to access, review and collect data from employee-owned devices.
    - ❑ Include the right to migrate all relevant data when employees upgrade their equipment.
- ❑ Integrate HR, IT & Legal management systems.
    - ❑ HR employee management (portal).
    - ❑ IT identity management (active directory).
    - ❑ Legal Hold/Matter management.
- ❑ Establish text tagging procedures to expedite future identification.
    - ❑ Tag the thread by adding "CompanyName Confidential" in the body of the conversation.
- ❑ Enroll all smartphones into a remote collection system such as ModeOne.
- ❑ Identify high-risk departments/employee levels via HR system.
    - ❑ IP, Financial, C-level, etc.
- ❑ Perform periodic collections and archive data for custodians or groups of employees deemed high-risk (if applicable to your industry).
    - ❑ Or wait for a legal hold to collect and archive.
    - ❑ Or collect once you become aware of an impending exit.
- ❑ Provide employee training on data privacy, cyber security threats, and other relevant practices.

Contact ModeOne for consultation and assistance. info@modeone.io

ModeOne

13-Steps to Mitigate Risks
of Employee BYOD Cell Phone Usage

REACTIVE STEPS

- ❑ HR, Legal and IT must collaborate.
  - ❑ Identify collection capabilities.
  - ❑ Identify Legal Holds, and take the necessary steps if the employee's data is subject to a hold.
  - ❑ Turn off all accounts at a specified time.
- ❑ Activate the ModeOne remote collection tool.
  - ❑ Collect upon notification of the exit.
  - ❑ Collect again at the exit interview.
  - ❑ Search for text tags to identify sensitive info on the device outside the protected zone.

Nothing can guarantee the safety of your information.
You can reduce the risks associated with
employee exits by following these 13 steps.

The ModeOne Advantage
Fast, Remote, Targeted, Cost-Effective, Global, and Secure

ModeOne