

# INGOLD SOLUTIONS GMBH

## Mobile Device Policy (Ref No: - ISMS/ IS/5.2/01)

### Purpose-

This policy outlines the use of mobile devices by employees of **INGOLD SOLUTIONS GMBH**

This policy should be read and understood by all employees who:

- ☐ Use a INGOLD SOLUTIONS GMBH owned mobile device
- ☐ Bring a personal mobile device onto INGOLD SOLUTIONS GMBH property

### Policy-

#### Use of Personal Mobile Devices-

Employees may have the opportunity to use their personal devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include, but are not limited to, personally owned cell phones, tablets, laptops and computers.

Employees who have not received authorization in writing from management and who have not provided written consent will not be permitted to use personal devices for work purposes. Failure to follow policies and procedures may result in disciplinary action up to and including termination of employment.

#### Use of INGOLD SOLUTIONS GMBH Owned Mobile Devices-

Certain employees may be issued a INGOLD SOLUTIONS GMBH owned mobile device based on job roles and responsibilities but the device remains the sole property of INGOLD SOLUTIONS GMBH.

### Security-

Employees must put a PIN, password or other security measures in place on every device that is used to access INGOLD SOLUTIONS GMBH information. Further, employees are required to have mobile device management (MDM) software installed on their personal mobile devices as recommended by PDS INFOTECH. This software will [list what the software does here, e.g., monitor all emails, text messages and photos, along with the physical location of the device. This software must be installed by the IT department prior to using the device for work purposes.

When possible, employees should use two-factor or two-step verification for added application/device security.

# INGOLD SOLUTIONS GMBH

Employees may not use any cloud-based apps or backup that allows INGOLD SOLUTIONS GMBH-related data to be transferred to unsecure parties (see “approved app list” at the end of this document). Due to security issues, mobile devices may not be synchronized to other devices in the employee’s home. Making any modifications to the device hardware or software, or installing additional hardware or software, beyond authorized and routine installation updates is prohibited unless approved by the IT department. Employees may not use unsecure Internet sites.

Employees whose personal devices have camera, video, or recording capability are restricted from using those functions anywhere in the building or on INGOLD SOLUTIONS GMBH property at any time unless authorized in advance by management.

An employee may not store information from or related to former employment on the INGOLD SOLUTIONS GMBH’s device.

## **Behavior-**

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of INGOLD SOLUTIONS GMBH devices. INGOLD SOLUTIONS GMBH policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to the use of personal devices for work-related activities.

Excessive personal calls, e-mails, or text messaging during the work day, regardless of the device used, can interfere with employee productivity and be distracting to others. Employees must handle personal matters on non-work time and ensure that friends and family members are aware of the policy. Exceptions may be made for emergency situations and as approved in advance by management.

Mobile devices shall be turned off or set to silent or vibrate mode during meetings, conferences, and in other locations where incoming calls may disrupt normal workflow.

## **Work Hours-**

Nonexempt employees may not use their mobile devices for work purposes outside of their normal work schedule without authorization in advance from management.

This includes but is not limited to reviewing, sending, and responding to e-mails or text messages, responding to calls or making calls.

Employees may not use their personal devices for work purposes during periods of unpaid leave without authorization from management. **INGOLD SOLUTIONS GMBH** reserves the right to deactivate the INGOLD SOLUTIONS GMBH’s application and access on the employee’s personal device during periods of unpaid leave.

## **Privacy-**

# INGOLD SOLUTIONS GMBH

No employee should expect any privacy except that which is governed by law. **INGOLD SOLUTIONS GMBH.** has the right, at any time, to monitor and preserve any communications that utilize **INGOLD SOLUTIONS GMBH.** networks in any way, including data, voicemail, telephone logs, Internet use, network traffic, etc., to determine proper utilization, regardless of the ownership status of the device used to access the INGOLD SOLUTIONS GMBH's networks. Management reserves the right to review, retain, or release personal and INGOLD SOLUTIONS GMBH-related data on mobile devices to government agencies or third parties during an investigation or litigation. Management may review the activity and analyze usage patterns and may choose to publicize this data to assure that **INGOLD SOLUTIONS GMBH.** resources in these areas are being utilized according to this policy. Furthermore, no employee shall knowingly disable any network software or system identified as a monitoring tool.

## **Inspection-**

At any time, the employee may be asked to produce the mobile device for inspection. The purpose of these inspections is to insure that the employee is following INGOLD SOLUTIONS GMBH policy.

## **Safety-**

Employees are expected to follow applicable state or federal laws or regulations regarding the use of electronic devices at all times.

Employees whose job responsibilities include regular or occasional driving are expected to refrain from using their mobile devices while driving. Regardless of the circumstances, including slow or stopped traffic, employees are required to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or texting. The only exception to this stipulation is if the call can be placed or accepted entirely hands-free. Special care should be taken in situations where there is traffic, inclement weather, or unfamiliar areas.

Employees who are charged with traffic violations resulting from the use of mobile devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas must refrain from using mobile devices as doing so can potentially be a major safety hazard.

## **Lost, Stolen, Hacked, or Damaged Equipment**

Employees are expected to protect mobile devices used for work-related purposes from loss, damage, or theft. In an effort to secure sensitive INGOLD SOLUTIONS GMBH data, employees are required to have remote wipe software (MDM) installed on their mobile devices by the IT department prior to using the devices for work purposes. This software allows all data to be erased remotely in the event the device is lost or stolen. The remote wipe process will remove all programs and data from the phone and reset it to factory defaults. **INGOLD SOLUTIONS**

# INGOLD SOLUTIONS GMBH

**GMBH.** will not be responsible for loss or damage of personal applications or data resulting from the use of INGOLD SOLUTIONS GMBH applications or remote wiping. Employees must notify management immediately in the event their mobile device is lost or stolen.

If the mobile device is damaged, the employee must notify management immediately. The employee will be responsible for the cost of repair or replacement.

Employees may receive disciplinary action up to and including termination for damage to INGOLD SOLUTIONS GMBH owned mobile devices caused willfully by the employee.

## **Termination of Employment**

Upon resignation or termination of employment, the mobile device will be reset to factory defaults using the remote wipe software. **INGOLD SOLUTIONS GMBH** will not be responsible for loss or damage of personal applications or data resulting from the remote wipe.