INGOLD SOLUTIONS GMBH

Remote Work Policy (Ref No: - ISMS/IS/5.2/20)

Purpose

The purpose of this policy is to establish the rules and conditions under which short and long-term telecommuting may occur in order to maintain acceptable practices regarding the use and protection of INGOLD SOLUTIONS GMBH **Information Resources**.

Audience

The INGOLD SOLUTIONS GMBH Remote Work Policy (Ref No: - ISMS/IS/5.2/20) applies to any individual connecting remotely to INGOLD SOLUTIONS GMBH information resources.

Policy

General Requirements

- Personnel must be approved by their manager and IT prior to remote access or teleworking. Under no circumstance is a person permitted to work remotely without prior permission.
- Personnel are responsible for complying with INGOLD SOLUTIONS GMBH policies when working using INGOLD SOLUTIONS GMBH **Information Resources** and/or on INGOLD SOLUTIONS GMBH time. If requirements or responsibilities are unclear, please seek assistance from the Security Committee. (duplicate from AUP)
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on INGOLD SOLUTIONS GMBH time and/or using INGOLD SOLUTIONS GMBH **Information Resources** are the property of INGOLD SOLUTIONS GMBH. (duplicate from AUP)
- The teleworker is responsible to ensure that non-employees do not access INGOLD SOLUTIONS GMBH data, including in print or electronic form.
- The team member will be required to maintain a regular schedule. All hours of work must be recorded according to regular INGOLD SOLUTIONS GMBH policies. Overtime and time off must have advance approval according to the regular policies of INGOLD SOLUTIONS GMBH.
- Equipment and information must be protected according to their classification and in alignment with the Information Classification and Management policy. Teleworkers are responsible for protecting INGOLD SOLUTIONS GMBH equipment and information from theft, damage, or other loss while in transit or at the remote work location. At no time should documents or INGOLD SOLUTIONS GMBH equipment be left unattended in a public area.
- Personnel are expected to follow INGOLD SOLUTIONS GMBH's Incidental Use policy when using INGOLD SOLUTIONS GMBH devices remotely.

Internet Connection

- Personnel must not connect to an unsecured Wi-Fi network with INGOLD SOLUTIONS GMBH equipment or to perform INGOLD SOLUTIONS GMBH work.
- Wi-Fi connections must be secured with strong encryption (WPA2). The use of WPA or WAP is not allowed.
- When connecting to a Wi-Fi network, personnel must use only the pre-approved VPN solution.
- Users must not connect to another wireless network and the INGOLD SOLUTIONS GMBH wireless network simultaneously.
- The use of split-tunnel VPN is prohibited.
- For long-term or home office networks:
    - A high-speed Internet connection is required. Personnel will provide the Internet service at their own expense. The internet connection must be of sufficient bandwidth to allow the team member to efficiently perform their regular job functions.
    - IT will determine if the person's network is secure or whether a INGOLD SOLUTIONS GMBH issued wireless router will be needed OR teleworkers will comply with [Teleworking Procedures] for implementing wireless networks securely.
    - Wireless networks must be secured with a strong password, consisting of 16 or more characters.
    - When possible, the home network used with INGOLD SOLUTIONS GMBH Information Resources should be isolated from other devices and computers in the home.

Equipment

- Only INGOLD SOLUTIONS GMBH provided computing devices, such as desktops and laptops, may be used for working remotely.
- Computing devices must be secured with INGOLD SOLUTIONS GMBH provided or approved:
    - Active and up-to-date antivirus software
    - Active local firewall
    - Full-disk encryption
    - Automatic screen lock
- Personnel are responsible for regularly rebooting their device in order to allow software patches and updates to be installed.
- Personally owned devices, including but not limited to USB memory, portable hard drives, mobile phones, MP3 players, iPods/iPads, and smart gadgets, are not allowed to be connected to INGOLD SOLUTIONS GMBH equipment, including wireless connections.
- Maintenance of INGOLD SOLUTIONS GMBH provided equipment must be provided or preapproved by IT.

Printing

- The printing of any non-public INGOLD SOLUTIONS GMBH information must be preapproved by the Information Owner.
- The printing of any non-public INGOLD SOLUTIONS GMBH information to a public printer is prohibited.
- Personnel must be preapproved by IT Technology and their manager for printing at a remote location. Personnel approved to print must have (or be supplied with) a shredder.
    - IT will determine if the person's network is secure or whether a INGOLD SOLUTIONS GMBH issued wireless router will be needed.
    - The device used to print must be directly connected to the printer used. Wireless printing must be pre-approved by Information Technology and requires the use of strong encryption.
- All non-public INGOLD SOLUTIONS GMBH information must be secured when not in use and shredded when no longer needed in accordance with INGOLD SOLUTIONS GMBH's Information Classification and Management policy.
- The printing of Confidential information at a remote location is not permitted.

Telephone

- Remote personnel must use the INGOLD SOLUTIONS GMBH provided phone or headset for all INGOLD SOLUTIONS GMBH related calls.
- When other people are present in the remote work location, a headset must be used to safeguard the conversation.

Office Requirements

- Workspaces must be secured to protect all INGOLD SOLUTIONS GMBH equipment and maintain the confidentiality of all information related to the organization and/or its customers.
- Personnel must allow IT to inspect and/or retrieve the equipment provided to them at any time.
- The INGOLD SOLUTIONS GMBH may inspect and/or retrieve any INGOLD SOLUTIONS GMBH information maintained at home by personnel.
- The use of personal video surveillance on home entrances and exits is encouraged.