ISO27001

BITS Technology Group

2022 Mobile Devices and Teleworking Policy

v1.0.3

Published On: Mon Jan 20 2025 16:00:44 GMT+1000 (Australian Eastern Standard Time)

Last Reviewed: Mon Jun 09 2025 09:10:00 GMT+1000 (Australian Eastern Standard Time)

Policy Owner: Bernard Mangelsdorf

Please note: This policy is an extract from the de.iterate policy reader. For the best viewing experience we recommend reading this policy in the native de.iterate policy reader. This policy was exported from de.iterate on 9/6/2025 by Esther Mangelsdorf esther.mangelsdorf@bitsgroup.com.au

Screen 1 Details

To ensure security is maintained when working remotely and on the go

Mobile Devices

Control IDs: A.8.1, A.6.7

- Mobile devices enable flexible working conditions. However, flexible working conditions do not mean flexible security conditions. BITS Technology Group maintains the same level of information security no matter where the data is being accessed or by what device.
- It is up to each user at BITS Technology Group to understand the classification of the data they are working on and continuously assess their working conditions to make sure they are operating within BITS Technology Group policies and guidelines for Acceptable Use, Access Control, Secure Areas, and Secure Handing of Data.

Hint: When working in public spaces, do not work on Customer Confidential or Business Confidential data

ISO27001

BITS Technology Group

2022 Mobile Devices and Teleworking Policy

v1.0.3

Published On: Mon Jan 20 2025 16:00:44 GMT+1000 (Australian Eastern Standard Time)

Last Reviewed: Mon Jun 09 2025 09:10:00 GMT+1000 (Australian Eastern Standard Time)

Policy Owner: Bernard Mangelsdorf

Please note: This policy is an extract from the de.iterate policy reader. For the best viewing experience we recommend reading this policy in the native de.iterate policy reader. This policy was exported from de.iterate on 9/6/2025 by Esther Mangelsdorf esther.mangelsdorf@bitsgroup.com.au

Screen 2 Details

To ensure security is maintained when working remotely and on the go

BYO Devices

Control IDs: A.8.1, A.6.7

- All devices supplied by BITS Technology Group come with inherent security controls enabled. These controls are not to be disabled without the explicit permission of BITS Technology Group.
- When working on remote private Wi-Fi networks is important staff do not allow other users on the network to use company devices or devices accessing company information for non-BITS Technology Group business.
- All devices must use a complex passcode and biometric logins where availablebrAll staff who intend to use their personal devices for work, referred to as 'Bring Your Own Device' or BYOD which are used to access BITS Technology Group information is required to meet minimum security standards listed below:brAll devices must have at-rest encryption enabled

Hint: When working in flexible environments, all users must use personal Wi-Fi hotspots or designated private networks

ISO27001

BITS Technology Group

2022 Mobile Devices and Teleworking Policy

v1.0.3

Published On: Mon Jan 20 2025 16:00:44 GMT+1000 (Australian Eastern Standard Time)

Last Reviewed: Mon Jun 09 2025 09:10:00 GMT+1000 (Australian Eastern Standard Time)

Policy Owner: Bernard Mangelsdorf

Please note: This policy is an extract from the de.iterate policy reader. For the best viewing experience we recommend reading this policy in the native de.iterate policy reader. This policy was exported from de.iterate on 9/6/2025 by Esther Mangelsdorf esther.mangelsdorf@bitsgroup.com.au

Screen 3 Details

To ensure security is maintained when working remotely and on the go

Minimum Security Standards (continued)

Control IDs: A.8.1, A.6.7

- All devices must auto-lock after an idle period of no more than 1 minute
- Before accessing BITS Technology Group systems, all devices must have a BITS Technology Group 'Mobile Device Management' policy installed on them. This enables BITS Technology Group to set the above settings, and erase sensitive company information from the device if it's lost or stolen.
- All users who BYO Devices must have signed their employment contract, which acknowledges the users' duties to protect information and waives any right to business data stored on the device.
- All software in use on BYO Devices for business purposes must be appropriately licensed for your use case.
- All devices which support BITS Technology Group Antivirus and Antimalware technology should have it installed and running.

Hint: Don't be fooled, someone else's WiFi is never free