sensible

BYO (Bring Your Own) Device Policy

Definition

Due to the ever increasing and sophistication of malware and sensitivity of organisational data that may be lost due to data leakage and due to increased costs of the growing usage in BYOD devices, the following policy now applies to all BYOD Devices.

Sensible defines a BYOD device as any device, which is used for company purposes but not owned by the supported organisation.

Criteria

Device types included in this policy:

- Computers
- Mobile Phones
- Tablets
- Printers
- Wi-Fi devices
- Other Network devices

Policy statement

Sensible aims to enforce security protocols to ensure that BYOD devices brought on to supported client organisation networks do not negatively impact client operations. Ensuring that devices are introduced with appropriate security/configuration requirements minimises client's exposure to data leakage and any impact to business operations.

Acceptable Use

- Devices approved by Sensible (in advance) may be allowed to be connected directly to any supported network infrastructure.
- These devices must first be authorised by client management in writing to Sensible.
- Any device that is lost or stolen must be reported to Sensible and company management immediately.
- All devices will only be given short term temporary access. At the expiry of this term, all the conditions in this policy need to be repeated.
- Support is limited to client's approved applications and basic connectivity only and does not extend to home or public network configurations or applications or data installed for personal use.
- No organisational data and/or software is to be stored on personal devices without written authorisation from client management.
- The security, integrity and retention of any client data stored on approved BYOD devices is the responsibility of the individual.
- All devices accessing corporate resources and or used for business communications must meet the following security requirements:

i) All Sensible policies and procedures are to be followed at all times
ii) All client policies and procedures are to be followed at all times
iii) If Connecting to cabled office network:
    (1) Sensible's approved security and anti-malware software to be installed and always operational
    (2) Sensible has a fully operational, dedicated full administrator account on the device
    (3) Sensible's monitoring tools are deployed to the device and always operational
    (4) All latest software security updates are installed
    (5) Sensible has conducted a security audit of the device in advance
iv) Connected to Wireless networks:
    (1) If not segregated from the wired network by using VLAN's, etc., then the cabled policy above applies.
    (2) If segregated, only public internet access is possible.
v) Mobile Devices restrictions
    (1) All devices must be secured via password and pin combination
    (2) In the event where a remote wipe is required, the company reserves the right to enact the remote wipe process. The end-user acknowledges that the act of remote wipe may delete more than only company data. This is a known and agreed upon risk.
vi) Any Setup and Ongoing costs of the above to be accepted and charged separately to the client
vii) All support incidents related to this device to be accepted and charged separately to the client
viii) Support is limited to the applications covered under the normal support agreement for corporate-owned devices for the client.
ix) VPN/FTP/File Sharing software access is not allowed from BYOD devices, unless Sensible's Mobile Device Management Software is also deployed (in advance).

Sensible reserves the right to refuse support and connection of any device that does not comply with the above criteria.

Breaches

- Individuals must comply with the terms of this policy in conjunction with any other relevant client employment policies, codes of conduct and/or statutory or other legal obligations. Failure to comply with these terms may result in:
    - Disciplinary action taken against the individual by client management up to and including termination of employment.
    - The incursion of additional costs and damages by the client and/or Sensible in remediating works resulting from the breach of security and/or data protection measures. Legal action may be taken against the individual depending on the circumstances and intent of the breach.

Limitation of Liability

Sensible does not accept any liability for any damage caused by any BYOD device.