Bring Your Own Device (“BYOD”) Policy

MIoD grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. MIoD reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the MIoD’s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

MIOD employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of the MIOD.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Accessing or distributing pornographic or other unsuitable material is strictly prohibited and may constitute serious misconduct.
- Devices may not be used at any time to:
  - Store or transmit illicit materials;
  - Store or transmit proprietary information belonging to another company;
  - Harass others or partake in any inappropriate behaviour;
  - Engage in outside business activities.
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.

Devices and Support

- Smartphones are allowed.
- Tablets such as iPads and Android tablets are allowed.
- MIoD IT provides connectivity support where possible.
- Devices must be presented to MIoD ITfor proper configuration before access to the network can be provided.

Reimbursement

- The company will not reimburse the employee for the cost of the device and any allowances for such equipment are subject to individual contractual arrangements as per the needs of job holder.

Security

- In order to prevent unauthorised access, devices must be password-protected in line with the MIoD's Password Security Policy.
- Smartphones and tablets belonging to employees that are for personal use only are/are not allowed to connect to the network.

Risks/Liabilities/Disclaimers

- While MIoD IT will take every precaution to prevent the employee's personal data from being lost, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Employees are responsible for insuring their own devices and the MIoD will take no responsibility for lost or stolen devices
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- The MIoD reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with this policy.