Information security policy

BYOD (Bring Your Own Device)

Policy summary
Employees who prefer to use their personally-owned IT equipment for work purposes must be explicitly authorized to do so, must secure corporate data to the same extent as on corporate IT equipment, and must not introduce unacceptable risks (such as malware) onto the corporate networks by failing to secure their own equipment.

Applicability
This policy forms part of the corporate governance framework. It is particularly relevant to employees who wish to use PODs (see below) for work purposes. This policy also applies to third parties acting in a similar capacity to our employees whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies.

Policy detail
Background
In contrast to Information and Communications Technology (ICT) devices owned by the organization, Personally Owned Devices (PODs) are ICT devices¹ owned by employees or by third parties (such as suppliers, consultancies and maintenance contractors). Authorized employees and third parties may wish to use their PODs for work purposes, for example making and receiving work phone calls and text messages on their own personal cellphones, using their own tablet computers to access, read and respond to work emails, or working in a home-office.

Bring Your Own Device (BYOD) is associated with a number of information security risks such as:

- Loss, disclosure or corruption of corporate data on PODs;
- Incidents involving threats to, or compromise of, the corporate ICT infrastructure and other information assets (e.g. malware infection or hacking);
- Noncompliance with applicable laws, regulations and obligations (e.g. privacy or piracy);
- Intellectual property rights for corporate information created, stored, processed or communicated on PODs in the course of work for the organization.

Due to management’s concerns about information security risks associated with BYOD, individuals who wish to opt-in to BYOD must be authorized by management and must explicitly accept the requirements laid out in this policy beforehand. Management reserves the right not to authorize individuals, or to withdraw the authorization, if they deem BYOD not to be appropriate and in the best interests of the organization. The organization will continue to provide...

¹ PODs are typically laptops, tablet computers, ultra-mobile PCs (UMPCs), desktop PCs, Personal Digital Assistants (PDAs), palmtops, cellphones, smartphones, digital cameras, digital memo recorders, printers etc., plus the associated portable storage media such as USB memory sticks, memory cards, portable hard drives, floppy disks etc.
its choice of fully owned and managed ICT devices as necessary for work purposes, so there is no compulsion for anyone to opt-in to BYOD if they choose not to participate in the scheme.

Policy axioms (guiding principles)
A. The organization and the owners and users of PODs share responsibilities for information security.
B. Nothing in this policy affects the organization’s ownership of corporate information, including all work-related intellectual property created in the course of work on PODs.

Detailed policy requirements
1. Corporate data can only be created, processed, stored and communicated on personal devices running the organization’s chosen Mobile Device Management (MDM) client software. Devices not running MDM (including devices that cannot run MDM, those on which the owners decline to allow IT to install MDM with the rights and privileges it needs to operate correctly, and those on which MDM is disabled or deleted after installation) may connect to designated guest networks providing Internet connections, but will not be granted access to the corporate LAN. They must not be used to create, modify, store or communicate corporate data.

2. PODs must use appropriate forms of device authentication approved by Information Security, such as digital certificates created for each specific device. Digital certificates must not be copied to or transferred between PODs.

3. BYOD users must use appropriate forms of user authentication approved by Information Security, such as userIDs, passwords and authentication devices.

4. The following classes or types of corporate data are not suitable for BYOD and are not permitted on PODs:
   - Anything classified SECRET or above;
   - Other currently unclassified but highly valuable or sensitive corporate information which is likely to be classified as SECRET or above;
   - Large quantities of corporate data (i.e. greater than 1 Gb in aggregate on any one POD or storage device).

5. The organization has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete corporate data without reference to the owner or user of the POD.

6. The organization has the right to seize and forensically examine any POD believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.

7. Suitable antivirus software must be properly installed and running on all PODs.

8. POD users must ensure that valuable corporate data created or modified on PODs are backed up regularly, preferably by connecting to the corporate network and synchronizing the data between POD and a network drive, otherwise on removable media stored securely.

9. Any POD used to access, store or process sensitive information must encrypt data transferred over the network (e.g. using SSL or a VPN) and while stored on the POD or on separate storage media (e.g. using TrueCrypt), whatever storage technology is used (e.g. hard disk, solid-state disk, CD/DVD, USB/flash memory stick, floppy disk etc.).

10. Since IT Help/Service Desk does not have the resources or expertise to support all possible devices and software, PODs used for BYOD will receive limited support on a ‘best endeavors’ basis for business purposes only.

11. While employees have a reasonable expectation of privacy over their personal information on their own equipment, the organization’s right to control its data and manage PODs may
occasionally result in support personnel unintentionally gaining access to their personal information. To reduce the possibility of such disclosure, POD users are advised to keep their personal data separate from business data on the POD in separate directories, clearly named (e.g. “Private” and “BYOD”).

12. Take care not to infringe other people’s privacy rights, for example do not use PODs to make audio-visual recordings at work.

Responsibilities

- **Information Security Management** is responsible for maintaining this policy and advising generally on information security controls. It is responsible for issuing digital certificates to authenticate authorized PODs, and for monitoring network security for unauthorized access, inappropriate network traffic etc. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the obligations identified in this policy.

- **IT Department** is responsible for managing the security of corporate data and configuring security on authorized PODs using MDM. IT is also explicitly responsible for ensuring the security of the MDM software and related procedures in order to minimize the risk of hackers exploiting MDM to access mobile devices.

- **IT Help/Service Desk** is responsible for providing limited support for BYOD on PODs on a ‘best endeavors’ basis for work-related issues only. Information security incidents affecting PODs used for BYOD should be reported promptly to IT Help/Service Desk in the normal way.

- **All relevant employees** are responsible for complying with this and other corporate policies at all times.

- **Internal Audit** is authorized to assess compliance with this and other corporate policies at any time.

Related policies, standards, procedures and guidelines

<table>
<thead>
<tr>
<th>Item</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security policy manual</td>
<td>Defines the overarching set of information security controls reflecting ISO/IEC 27002, the international standard code of practice for information security management</td>
</tr>
<tr>
<td>Mobile/portable computing policy</td>
<td>Specifies a number of information security controls applicable to the use of mobile and portable devices. Although it was</td>
</tr>
<tr>
<td>MDM standards and procedures</td>
<td>Given stringent information security requirements and the diverse nature of mobile/portable devices, the choice, installation, configuration and use of Mobile Data Management software is non-trivial. IT’s responsibilities are fulfilled through MDM technical standards and operating procedures.</td>
</tr>
<tr>
<td>Information Asset Ownership policy</td>
<td>Information Asset Owners are responsible for classifying their assets and may determine whether BYOD is or is not appropriate for them.</td>
</tr>
<tr>
<td>Human Resources policies, procedures, code of conduct etc.</td>
<td>Explain standards of behavior expected of employees, and disciplinary processes if the rules are broken.</td>
</tr>
</tbody>
</table>
### Contacts

For further information about this policy or general advice on information security, contact the IT Help/Service Desk. Security standards, procedures, guidelines and other materials supporting and expanding upon this and other information security policies are available on the intranet Security Zone. The Information Security Manager can advise on more specific issues.

---

**Important note from IsecT Ltd.**

This policy is unlikely to be entirely sufficient or suitable for you without customization. This is a generic model or template policy incorporating a selection of common controls in this area derived from our knowledge of good security practices and international standards. It does not necessarily reflect your organization’s specific requirements. We are not familiar with your particular circumstances and cannot offer tailored guidance. It is not legal advice. It is meant to be considered by management as part of the security awareness program, ideally as part of the regular review and update of your information security policies.

For the Word version of this and over 40 other security policies, see [www.NoticeBored.com](http://www.NoticeBored.com).