|  |  |  |
| --- | --- | --- |
| Document ID  **ITSD109** | Title  **BYOD POLICY** | Print Date  **mm/dd/yyyy** |
| Revision  **0.0** | Prepared By  **Preparer’s Name / Title** | Date Prepared  **mm/dd/yyyy** |
| Effective Date  **mm/dd/yyyy** | Reviewed By  **Reviewer’s Name / Title** | Date Reviewed  **mm/dd/yyyy** |
|  | Approved By  **Final Approver’s Name / Title** | Date Approved  **mm/dd/yyyy** |

|  |  |
| --- | --- |
| **Policy:** | Company employees and contractors may use their personal electronic devices (e.g., smartphones, tablets) for conducting company business, provided that they understand and agree with the “Bring Your Own Device” (BYOD) policy, have been granted express permission, and act in accordance with the policy. |
| **Purpose:** | To communicate specific standards and guidelines regarding the use of personal devices to conduct company business. |
| **Scope:** | This policy applies to all Company personnel and their personal electronic devices. |
| **Responsibilities:** | All Employees are responsible for being aware of, understanding, and adhering to the Company’s BYOD policy. |
|  | Department Managers are responsible for communicating BYOD policy updates to the employees in their respective departments. |
|  | The Human Resources Manager is responsible for communicating the BYOD policy to new employees and retaining employee policy acknowledgements. |
|  | The Information Security Manager monitors BYOD usage and enforces the BYOD policy. |
|  | The Information Technology Manager (IT Manager) is responsible for developing BYOD policy and for reviewing the policy and any changes to it with the Policy Committee. The IT Manager also oversees monitoring and enforcement of the BYOD policy. |
|  | The Policy Committee is responsible for review and final approval of the Company’s BYOD policy and subsequent updates. |
| **Definitions:** | BYOD – ***B***ring ***Y***our ***O***wn ***D***evice, or using one’s personal mobile phone, PC, tablet, or other personal electronic device to conduct the Company’s business. |
|  | Policy Committee – A group comprised of Top Management and the IT Manager. The purpose of the Policy Committee is to develop, review, approve, and revise the Company’s BYOD policy, as needed. |
|  | Top Management – A group comprised of the Company’s chief executive and chief financial officer, at a minimum. In larger companies, top management may include department / functional managers (e.g., VP-Sales, CTO). |

**Procedure:**

### 1.0 BYOD POLICY DEVELOPMENT

1.1 The Information Technology (IT) Manager shall develop the Company BYOD policy, which may be based on common business standards and practices and on legal/regulatory requirements (see Reference B).

It is important to understand the myriad considerations for a BYOD policy within this very dynamic technology space, in order to properly protect your corporate technology infrastructure. Don’t take this step lightly. The BYOD Policy needs to take into account:

* The company’s technology infrastructure;
* Roles and responsibilities of various support services;
* Education, use, and operation of BYOD devices;
* Security risks;
* Ethical and legal considerations;
* Applications that may run on BYOD devices; and
* IT asset management.

This is not a complete list of BYOD factors; the Company may have to consider additional issues.

1.2 The IT Manager shall present the policy to the Policy Committee for review.

1.3 The Policy Committee shall review the BYOD policy, revise as needed, and signify its approval.

### 2.0 BYOD POLICY IMPLEMENTATION

2.1 Upon final approval of the BYOD policy, the IT Manager shall communicate the policy to all department managers. Department managers shall, in turn, communicate the policy to all employees in their respective departments.

* The Human Resources Manager shall be responsible for communicating the Company BYOD policy to all *new employees*.

2.2 All employees shall receive a copy of ITSD109-1 COMPANY BYOD POLICY ACKNOWLEDGEMENT. Upon reviewing the document, each employee shall sign and date their copy of the acknowledgement and return it to Human Resources. Employees should keep a copy of this document for themselves.

2.3 The IT Department shall manage records and documents used or generated by BYOD devices in accordance with Company procedures ITAD102 IT RECORDS MANAGEMENT and ITAD103 IT DOCUMENT MANAGEMENT.

2.4 The Information Security Manager shall monitor Company email, text messages, etc., for the purpose of enforcing the BYOD policy, as well as security policies.

### 3.0 BYOD POLICY review

3.1 At regular intervals (annually, at a minimum), the IT Manager shall review the Company’s BYOD policy to see if it continues to meet Company and other requirements (legal/regulatory, etc.).

3.2 If the BYOD policy does not adequately address Company and other requirements, the IT Managers shall convene the Policy Committee for the purpose of implementing revisions to the policy.

### 4.0 BYOD POLICY CHANGES

4.1 The Policy Committee shall periodically review the Company’s BYOD policy, to verify that it continues to meet Company requirements. Implementation of the BYOD policy needs to be an iterative process, due to the changing nature of technology and how it impacts the Company and the general business environment.

4.2 Where the policy does not meet requirements, the Policy Committee shall revise the policy as needed and communicate the revised policy to the IT Manager, who is responsible for its implementation and distribution.

4.3 Within one month of such changes to the BYOD policy, the IT Manager shall verify that they have been implemented and are having the desired effect.

**Forms/Records:**

* ITSD109-1 BYOD POLICY & ACKNOWLEDGEMENT

**References:**

1. **ISO 9001:2008, QUALITY MANAGEMENT SYSTEMS - REQUIREMENTS**

Clause 4.2.4 of ISO 9001 states that the organization must establish and maintain records to provide *evidence of conformity to requirements*. Those requirements include legal and regulatory considerations, such as security and privacy. In addition, all records must remain legible, readily identifiable, and retrievable.

1. **SARBANES-OXLEY ACT OF 2002**

The Sarbanes-Oxley Act (or “SOX”) is designed in part to prevent manipulation, loss, and/or destruction of publicly-held companies’ records. Records used, stored, or generated by BYOD devices may be subject to inspection and retention guidelines. Therefore, it is important that publicly-held organizations consider implementing a BYOD policy to help ensure SOX compliance.

1. **A TOOLKIT TO SUPPORT FEDERAL AGENCIES IMPLEMENTING BRING YOUR OWN DEVICE (BYOD) PROGRAMS**

This is a product of the Digital Services Advisory Group and Federal Chief Information Officers’ Council, intended to serve U.S. government agencies considering implementation of BYOD programs. This Toolkit provides key areas for consideration and examples of existing policies and best practices.

In addition to providing an overview of considerations for implementing BYOD, the BYOD Working Group members developed a small collection of case studies to highlight the successful efforts of BYOD pilots or programs at several government agencies. The Working Group also assembled examples of existing policies to help inform IT leaders who are planning to develop BYOD programs for their organizations.

For details, see <http://www.whitehouse.gov/digitalgov/bring-your-own-device>.

**Additional Resources:**

A. ITAD102 IT RECORDS MANAGEMENT

B. ITAD103 IT DOCUMENT MANAGEMENT

C. ITSD102 IT SECURITY PLAN

D. ITSD105 COMPUTER MALWARE

# E. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, ISACA (2014) - <http://www.isaca.org/cobit/pages/default.aspx>.

**Revision History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Description of Changes** | **Requested By** |
| 0.0 | mm/dd/yyyy | Initial Release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

[This page intentionally left blank]

**ITSD109-1 BYOD POLICY & ACKNOWLEDGEMENT**

### 1.0 BYOD AND THE COMPANY

All portions of the Company information infrastructure, including the information being transported by this infrastructure, are the property of the Company. This includes all messages, documents, and data transmitted or received through the Company information infrastructure, which may be augmented by personal electronic devices

Since such messages, documents, and data are Company property, all BYOD-related accounts and any information used, exchanged, and stored by these accounts are subject to inspection at any time.

Personal portable devices are powerful tools that can greatly enhance communication and productivity. Use of personal devices, or BYOD, to conduct business within the following guidelines by Employees and contractors is encouraged. The Company reserves the right to revoke any employee’s or contractor's BYOD privilege for cause.

In the context of this document, “personal electronic device,” “personal device,” and “BYOD device” are synonymous.

### 2.0 BYOD GUIDELINES

Employees shall follow the following general guidelines concerning the use of personal devices:

* All use of BYOD devices are subject to the companies Acceptable Use Policy.
* Text messages, email, and other forms of information transmission by BYOD devices are not private. Messages transmitted via BYOD devices are the property of the Company and are subject to inspection at any time. Use of a personal portable device to access Company information automatically implies consent to search.
* User will not download or transfer sensitive business data to their personal devices. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a charge/complaint/case, proprietary information, or agency financial operations.
* Users will password-protect their devices.
* The user agrees to maintain the original device operating system and keep the device current with security patches and updates released by the manufacturer. The user agrees not to “jail break” (i.e., install software that allows them to bypass standard built-in security features and controls) their device.
* User agrees that they will not share their device with other individuals or family members, due to the business use of the device.
* BYOD users shall be required to retain emails, text messages, etc., related to essential or mission-critical projects; such records should be transferred to Company storage within two (2) business days. Messages or other transmissions that do not pertain to mission-critical projects or issues should be deleted when the Company no longer needs them.
* Because attachments to emails and messages are used to attack computers and systems – and because attachments occasionally use a lot of bandwidth – sending a file as an attachment and opening an attachment are discouraged.
* Personal devices shall not be used for commercial[[1]](#footnote-1) or political purposes.
* Employees shall ensure all communication, whether through Company email, messaging services, or their personal devices, is conducted in a professional manner. The use of vulgar, obscene, lewd, or suggestive language or the use of language or tone that could reasonably be construed as harassment, intimidation, or threats is prohibited.
* Company users shall not reveal private or personal information via their personal devices without specific, written authorization from management.
* Users should ensure that any messages they send via their personal devices are sent only to users with a specific need to know. The transmission of messages to large groups via personal device should be avoided.
* Personal devices shall not be used for any illegal or unlawful purpose, including transmission of violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful material.
* Personal devices shall not be used to harass, intimidate, or otherwise annoy anyone.
* The Company shall not be held liable for damages related to inappropriate use of personal devices by Employees, contractors, or their families.
* Failure to follow any part of this policy may result in disciplinary action, up to and including termination.

### 3.0 EMPLOYEE ACKNOWLEDGEMENT

I have reviewed the Company’s BYOD policy. By signing and dating this form, I attest to my understanding and acceptance of this policy. Furthermore, I understand that if I am ever found violating this policy, I may be subject to Company disciplinary action, up to and including termination, as well as civil and/or criminal prosecution.

Signature: Date:

Print name:

1. Aside from those of the Company [↑](#footnote-ref-1)