**Bring Your Own Device (BYOD) Policy**

BYOD policies can vary significantly from organization to organization depending on your priorities and concerns, and should be designed in consultation with HR, finance, legal and IT security teams. Ideally, an organization’s practices around BYOD should be detailed in a formal policy regarding the use of personal devices for work. While the temptation can be strong for IT to develop specific policies for every conceivable scenario, the reality is that most considerations can be addressed through the application of a few simple, consistent principles. In most cases, IT can think about how to manage and provide secure access to data and applications in terms of people, not the devices they use. You may want to define more granular policies regarding specific device types, network connections and locations, but these will typically represent a smaller and more manageable set of scenarios.

Defined in consultation with legal, finance, HR teams, BYOD policies identify the scenarios in which BYOD is allowed, whether a subsidy will be provided, how security and support will be handled and other factors. In developing your policy, you should be sure to consider the following areas.

**Eligibility:** Organizations should identify who can use personal devices for work and scenarios where it is inappropriate due to data security, worker type or other factors. In enterprises that allow a BYOD device to replace a corporate endpoint, this decision is typically optional for the worker, with managerial discretion over which team members are appropriate candidates.

**Allowed devices:** BYOD programs should allow people to use the best devices for their needs, from smartphones and tablets to Mac and Windows laptops. A device-independent strategy provides this level of freedom while giving IT the option to manage BYOD devices if they so choose.

**Service availability:** BYOD doesn’t have to be an all-or-nothing proposition. You should think about the services and apps you want to make available on BYOD devices and whether it differs by work groups, user types, device types and network utilized.

**Rollout and Acceptable Use:** Communication is vital to BYOD success. Provide guidance to help people decide whether to participate, what the right device is and to understand the responsibilities that come with bringing their own device, including how data can be accessed, used and stored. How policy violations and lost/stolen devices will be handled should also be determined.

**Cost sharing:** Some organizations provide a subsidy for BYOD devices and other services, especially in cases where a corporate device is no longer provided.

**Security:** For effective data protection and information governance, business information should reside on the endpoint only in isolated, encrypted form, and only when necessary. Network security can be maintained through granular policy-based user authentication, with full tracking and monitoring to support compliance and privacy. Control must also exist over data exfiltration concerns, such as print capabilities and client-side storage. IT should require antivirus/anti-malware software on all BYOD devices and consider remote wipe mechanisms if business information is allowed on the device.

**Support and maintenance:** BYOD policies should spell out the type of incidents IT will support as and the extent of support. Especially when a BYOD device is used in place of a corporate device, ***<Company Name>*** recommends maintaining a loaner pool of devices to allow uninterrupted productivity while the device is serviced. Consider providing executives and other key personnel with additional, concierge-style support.

**PLEASE NOTE**

This document is not intended to be a complete guide to establishing a bring-your-own-device (BYOD) policy for your organization, and the sample policy outlined below is not intended to be adopted as-is by any organization. ***<Company Name>*** recommends that your organization consult with your legal department and other stakeholders to define a policy that meets the unique needs of your organization and its operations. ***<Company Name>*** disclaims any and all liability for the use of this document and the considerations and policy outlined herein, either in whole or in part, in the definition and/or application of specific policies by any company or organization.

Recognizing that some employees prefer to use their own personal notebook and laptop for work, the company has introduced a bring-your-own-device (BYOD) program to provide this option. BYOD participants will be allowed to bring their own device to work for use in the office, and will also be offered a stipend to offset some of the cost of their device. All participants must meet program eligibility requirements and acknowledge and agree with the company’s BYOD policy as defined blow.

**Program Eligibility**

* Must be a full-time employee
* Requires manager approval
* Employee cannot be on a performance improvement plan at the time of applying for the BYOD program

**Policy**

* You must return your company-owned device to your cost center owner within 15 days of receiving your BYOD stipend. The IT Service Desk will assist in the transfer of files if required.
* The BYOD stipend will be charged against your cost center budget. Upon your acceptance into the program, a Status Change Form will be generated by the IT Service Delivery team and sent to HR and Payroll for payment processing. Your BYOD stipend will be paid to you in local currency within two payroll cycles following IT Service Delivery's approval of your admission into the program. Note that your BYOD stipend may be considered a form of income, and may be subject to customary tax withholdings.
* BYO smartphones running the following operating system versions are allowed: iPhone 4 or older, Android 4.3 or older, Blackberry 7 or older and Windows Phone 8.0 or older.
* BYO tablets including iPad and Android running minimum operating versions noted above are allowed.
* For BYO personal notebook or laptop computer:
  + BYOD Hardware, Operating System and Security Minimum Specifications
    - Hardware
      1. 80GB hard drive
      2. 2GB RAM
      3. 100Mbps Ethernet Card/Port
      4. “G” or “B” Wireless Card
      5. 2 GHz Processor
      6. Warranty support
    - Operating Systems
      * 1. Windows 7
        2. Mac OS X
    - Antivirus – provided by the company, installed locally on the device
* You do not have to purchase a new device to participate in the program. You can use your existing personal device that meets the minimum requirements as outlined in this policy.
* When using your device, you may access company information or information systems, including company applications and data, only by means of the company VPN/portal, and you should not access company information or information systems by any other method.
* Do not download or store any kind of confidential company information to your device or any personal, external storage device unless the data can be encrypted on the device. If you are uncertain whether it is permissible to download certain information, please review the BYOD Security Policy and contact the legal department for advice.
* Devices must be password protected with a strong password according to the company’s BYOD Security Policy.
* Smartphones and tablets must be enrolled in, managed and protected with company approved Enterprise Mobility Management product.
* Rooted (Android) or jailbroken (iOS) smartphones or tablets are strictly forbidden from accessing the company network.
* You may not download, install and use any app that does not appear on the company’s list of approved apps.
* If you become aware that the security of company information has been compromised, including by means of unauthorized disclosure or theft or loss of a device containing company information, immediately report such security breach to IT services.
* Please do not introduce inappropriate personal information into the company work environment. All applicable company policies, including the Anti-Harassment/Anti-Discrimination Policy andthe BYOD Security Policy, continue to apply to you.
* Your personal data on your BYO device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company’s data and technology infrastructure.
* Before enrolling in the program, in addition to the BYOD Security Policy, review the Corporate Security Policy in its entirety.
* You are responsible for supporting your device's hardware and personal apps.
* You are responsible for any costs incurred for servicing and repairing your device.
* In the event your device requires servicing or repairs by a third party vendor, the IT Service Desk will provide a loaner (standard Company laptop and image) for up to 10 business days.
* The company is not liable for theft, loss or damage to your device. If desired, you should arrange for insurance coverage at your own cost.
* Participation in the BYOD Program is for a two-year term for smartphones and tablets and a three-year term for laptops, and you must be in the program for a minimum of six months before being allowed to opt out of the program.
* In the event that you determine that this program is no longer suitable for you, or if you become ineligible for this program for any reason:
  + Please send email notification to <insert email> that you are no longer participating in the program.
  + You will be responsible for reimbursing ***<Company Name>*** at a prorated calculation of the BYOD allowance payment you received if you have not been enrolled in the program for more than one year.
  + You will be ineligible to participate in this program for two years (smartphones or tablets) or three years (laptops) from your opt-out or disqualification date.
* Employees are eligible to receive only one BYOD allowance payment per device every two years (smartphones or tablets) or three years (laptops). Upon the two-year anniversary of your enrollment in the program, you will be required to reapply for the program before receiving an additional BYOD allowance.
* Failure to comply with these requirements may result in termination from the BYOD Program and other disciplinary action.

**Employee Acknowledgement**

By electing to participate in the BYOD Program, I acknowledge and agree that:

* I shall at all times comply with the requirements of this policy;
* ***<Company Name>*** shall have no obligation to provide me with a Company-owned laptop, notebook or personal computer while participating in the BYOD Program;

The BYOD allowance may be considered income to me subject to customary tax withholdings; and

* If I am terminated from the program or from my employment (in each case either voluntarily or involuntarily) before the one-year anniversary of my enrollment in the program, I will be responsible for reimbursing to ***<Company Name>*** a pro-rata portion of the allowance payment made to me, and I authorize ***<Company Name>*** to deduct such amount from my wages, accrued vacation payment, incentive compensation owed to me, expense reimbursements or any other payment that is due to me either during my employment or upon the termination of my employment.

By clicking on the checkbox next to “I agree to the terms of the policy” on the enrollment page, you are electing to participate in the BYOD Program and an approval request automatically will be sent to your manager and the IT Service Delivery team.

**Source:**<https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&cad=rja&uact=8&ved=0ahUKEwj4jsbPiLvMAhVEJaYKHek2AjIQFghYMAY&url=https%3A%2F%2Fwww.citrix.com%2Fcontent%2Fdam%2Fcitrix%2Fen_us%2Fdocuments%2Fproducts-solutions%2Fdeveloping-your-byod-policy.docx&usg=AFQjCNHfZr1Kk8qymdPyIuwibL6lKYyoRA&bvm=bv.121070826,d.dGY>