This sample agreement and the material contained herein are for informational purposes only, and do not constitute legal advice or legal opinion. You should not act or rely on any information contained herein. BYOD (including wearables) and other employee device programs can vary significantly.

Sample Employee Agreement for Business Use of Employee-Owned Personal Computing Devices (Including Wearables[1])

Overview:
The Bring Your Own Device (BYOD) program allows employees to use their own computing devices for Company's business. This agreement allows employees to use their own small handheld devices, such as smart phones and approved wearables[2], for Company business. All of these are referred to herein as your "device". Participation in the BYOD programs is voluntary.

To access the Company WiFi service or Secure Mobile App services ("Services"), you must register the specific device to be used, select the applicable mobile device Services requested, and access terms of use specific to each Service[3], including privacy and information security obligations[4]. This agreement incorporates by reference the Service-specific terms of use provided on the Mobile Device Services website.

This agreement is between you and the Company entities authorized to govern or perform any of these terms. By clicking on the box at the end of this agreement, signing a physical copy of this agreement[5], or by accessing the Company network and using Company services on your device (such as email, contacts, etc.), you agree that you have read and accepted the terms and conditions in this agreement, as well as completed the device registration process further acknowledging your responsibilities and obligations.[6]

1. Eligibility

To be eligible to use your device under the BYOD programs, you must:

a. Be a regular Company employee (not a contingent or contract worker);

b. Register your device;

c. Ensure that your device meets minimum hardware and software specifications;

d. Be in a business group that allows participation in the program; and

e. Receive permission from your manager.

f. **If you breach any of the terms of this agreement, you may become ineligible to participate in the BYOD programs, and you may also be subject to disciplinary action.**

---

[1] Note: rather than try and keep up with all new types of computing devices, the agreement and related policies should govern the capabilities of the devices (e.g. recording capabilities) and generalize for all devices, as much as possible.
[2] Note: a company may decide that some wearables are approved for company use and some are not. You can insert a link to a website where approved devices are listed.
[3] Note: we have found that having one basic agreement such as this, plus a few service-specific terms located where the services are accessed on the internal portal, is better than a lengthier all-encompassing agreement that contains terms and conditions for services an employee isn't using, or multiple, somewhat repetitive agreements for each service, especially as different devices and services proliferate.
[4] Note: you can incorporate existing applicable privacy and information security policies into these terms & conditions as long as they conform and are kept updated.
[5] Note: in some jurisdictions, hard-copy (and possibly translated) agreements are required.
[6] Note: important clauses are in bold print.

2. Company Policies When Enrolled in the BYOD programs

a. When conducting Company business on your device, you must comply with all applicable laws and regulations as well as Company's policies and procedures. These include (but are not limited to) any of the following (or similar for your governing entity) policies that apply to you:

- *Company Code of Conduct;*
- *Company E-mail Policies;*
- *Company Computer Use Policies;*
- *Company Audio/Video Recording Policy;*
- *Company Information Security Policies and Procedures;*
- *Company Employment Agreement and Policies;*
- *Company Software Licensing Policy;*
- *Company Social Media Policy;*
- *Company Privacy Policies and Procedures;* and
- All other applicable Company policies and procedures.

b. In accordance with the Company Software Licensing Policy, when working on Company business, you may install and use on your device only legally acquired software for which you hold legally acquired and documented software licenses. Although Company may be licensed for a software product, that license may not extend to your device.

c. You may use your device for non-Company purposes during your personal time. However, you must exercise discretion in your personal use so as not to create legal liability for Company or negatively impact the working environment or resources of Company. Company is not responsible for the loss of any non-Company data or applications as a result of your personal use of your device on a Company network.

3. Information Storage and Backup

a. When possible, you must separate Company-owned information on your device from non-Company information. Various technologies may be available to you to support segregation of Company and non-Company information on your device depending upon its configuration and operating system.[7] You are responsible for implementing such technologies on your device as directed by Company.

b. You should back up any non-Company data you care about that is stored on your device. You should use a method that does not also capture Company data for storage.

c. If the Services accessed use encryption, you must not disable such encryption on your Device.

d. You must not access, view or store information classified as Company Highly Confidential on your Device.

4. Access to Company Network

You must not:

a. Allow anyone else to use your device when logged in to a Company network;

---

[7] Note: technology is advancing rapidly in its ability to partition off personal from work data on various computing devices. However, this is not yet possible on all types of mobile computing devices. This agreement is meant to be device-agnostic given the many new form factors in the market.

This sample agreement and the material contained herein are for informational purposes only, and do not constitute legal advice or legal opinion. You should not act or rely on any information contained herein. BYOD (including wearables) and other employee device programs can vary significantly.

b. Give anyone else your Company network login password; or

c. Give anyone else access to Company information on your device whether connected to the Company network or not.

5. Information and Device Management

a. **Your device is subject to standard Company information management policies and procedures including, but not limited to, a remote wipe that may remove all stored content to the extent technically feasible. A remote wipe may be performed as deemed necessary by Company. Examples of when a remote wipe may be necessary include, but are not limited to: employee termination, malicious code infection, lost or stolen device, or prolonged absence from Company. Company will attempt to selectively wipe only Company content unless you request a full wipe or a selective wipe is not technically feasible. However, Company is not responsible for any non-Company information lost as the result of a remote wipe.[8]**

b. Your device is subject to a software audit by Company on all installed software running on it (generally the software name, version, program file information, and license information), for purposes of standard Company software audit requirements.[9]

c. You must not disable or alter the settings for Company information security software or enforcement functions on your device.

6. Employees on a Litigation Hold Notice ("LHN") or Legal Compliance Hold Notice ("LCHN")

If you are, or become, subject to a LHN or LCHN, you must follow all LHN or LCHN instructions, take affirmative steps to preserve relevant information as instructed by Company Legal, and seek permission from Company Legal before removing any information from your device. You must notify Company if you leave the BYOD programs, stop a Service, or your employment with Company is terminated. Appropriate contact information will be supplied to you with any LHN or LCHN notifications. It is your responsibility to understand from the Company Legal team what services you are allowed to access on your device[10].

7. Hardware Support; Theft of, Loss of, or Damage to Your Device

a. You are responsible for the cost of all repairs and maintenance related to any device you own and choose to use at Company. In the event you require hardware support for your device you must use a reputable non-Company service center for repairs.

b. You must never provide your encryption password or Company login/passphrase to non-Company service center personnel. If your device password is required to perform the service, remove any Company information and access from your device prior to delivery to a non-Company service center. Once repairs have been completed you must change your encryption password, and Company recommends you change all passwords/passphrases.

---

[8] Note: a remote wipe should be proportional to the need. You should also check local laws regarding any potential company liability associated with a remote wipe that deletes employee personal data.

[9] Note: many enterprise software vendors are now seeking ways to audit all software use in an effort to sell additional licenses.

[10] Note: there may be Services you do not want accessed by an employee on a litigation or compliance hold.

This sample agreement and the material contained herein are for informational purposes only, and do not constitute legal advice or legal opinion. You should not act or rely on any information contained herein. BYOD (including wearables) and other employee device programs can vary significantly.

c. If your device is lost or stolen, you must immediately report the incident to Company Security at the earliest possible opportunity. Company will not compensate you if you bring a personal device to work and that device is lost, stolen or damaged. You are responsible for all costs and expenses related to use of your device at Company.

d. If your Device is lost, stolen, damaged, or stops working, you must take all steps necessary to continue to perform your job satisfactorily while your device is being replaced or repaired.

e. The BYOD programs are voluntary and offered for your convenience only. Company is not responsible for any malware infections or other malicious, or unauthorized, activities that result in compromise of your personal accounts or non-Company information. Company has no duty, and is not responsible for, network security for non-Company information. To avoid loss of non-Company information, you are responsible for maintenance of your non-Company information, device, and software.

8. Software Support

a. Company is not responsible for the backup and maintenance of non-Company information and software.

b. Company software support for your device will be limited to network protection, and connection to the Company network. To resolve other issues, you should use the Company BYO community self-support model located on Company's intranet site.

9. Travel and Physical Security

a. You must protect your device at least to the same level that Company employees are required by Company to protect Company-provided devices.

b. You must comply with all applicable export regulations pertaining to controlled technology, in particular when you travel to a controlled country with your device. Some countries may confiscate your device and examine the contents, including your non-Company information.

10. Non-Exempt Employee Guidelines

a. If you are an hourly or non-exempt employee, you are required to record and accurately report all time spent on Company business, regardless of the location or device used, including your device used under this agreement.

b. You may not perform Company work without reporting your time, even if overtime restrictions are in place. If you believe you are being asked to work without reporting your time or being properly compensated for time worked, you must immediately contact your Human Resources or Legal representative, or the Company Hotline, about the matter.

11. Compliance and Program Availability

a. Company reserves the right to terminate the BYOD programs at any time and for any reason. In addition, individual employees may be terminated from the program for any extended period of inactivity on the network. Employees may choose to terminate their participation in the BYOD programs at any time, under the terms of this agreement.

b. All the provisions of this section 11(b) are subject to Company's compliance with applicable law. Company reserves the right to search, intercept and review both incoming and outgoing email on your

This sample agreement and the material contained herein are for informational purposes only, and do not constitute legal advice or legal opinion. You should not act or rely on any information contained herein. BYOD (including wearables) and other employee device programs can vary significantly.

Company e-mail account on your device, all internet usage through a Company network on your device, and any Company information stored on your device. In addition, Company may investigate, copy and use any information from your device at the direction of a court, government agency or law enforcement agency, or when there is reasonable cause to suspect that there has been a violation of Company's Code of Conduct, Email Policies, or other Company information security or computer use guidelines, or a violation of other statutes or regulations. If requested by Company Corporate Security, Company Legal, Internal Audit, HR Legal, or Company Information Security, you must provide your device for manual inspection and possible copying and use of its content.

c. If, for whatever reason, you cease to be eligible to participate in the BYOD programs, you elect to cease your participation in the BYOD programs, you elect to remove a particular device from the BYOD program, or you leave employment with Company (whether voluntary or involuntary), you must give Company ten days' notice and deliver your device to IT Services for removal of Company information and applications. For certain BYOD devices, you may contact PC Services to remote wipe any Company information from your device.

d. Failure to follow these steps may result in disconnection from the Company network, or a remote wipe of your device that will remove all stored content, including your non-Company information.

   i. Company PC Services will remove your Company system access and all associated information and Company-provided applications.

   ii. As with a Company-provided computer, if you leave Company for any reason or are placed on a LHN or LCHN, Company PC Services will copy any Company information stored on your device. To the extent technically feasible, this will not include non-Company information unless legally required. This information will be stored securely by Company according to Company's standard data retention policies.

   iii. You may remove all non-Company information from your device before submitting it to Company PC Services, unless your device is subject to a LHN or LCHN as described above.

12. Updating This Agreement and Related Policies

a. This agreement and the Service-specific and other terms of use incorporated by reference herein constitute the entire agreement between you and Company, and supersede all prior agreements between you and Company concerning the subject matter herein.

b. Company may amend this agreement, or distribute and enforce new policies related to the BYOD programs, at any time without prior notice, provided that Company complies with all applicable laws. By continuing to participate in the BYOD programs, you agree to be governed by the terms and conditions as provided in the most updated version of this agreement and any related policies[11].

c. Company may deploy and enforce new policies without prior notice to address newly identified vulnerabilities. You agree to be governed by the terms and conditions as provided in such policies and to allow the installation of patches or software as deemed necessary by Company to protect Company information and the Company network. If your device does not support updated minimum security specifications, it may be disconnected from services when appropriate and remotely wiped to protect Company's information.

[11] Note: significant changes to the program or the Agreement should be managed by executing an updated agreement.

This sample agreement and the material contained herein are for informational purposes only, and do not constitute legal advice or legal opinion. You should not act or rely on any information contained herein. BYOD (including wearables) and other employee device programs can vary significantly.

13. Severability

If any provision of this agreement is determined by a court of competent jurisdiction to be invalid, illegal, or unenforceable, such determination will not affect the validity of the remaining provisions.

This agreement was updated _____, 2014.

<Insert forced scroll and clickable box, then track agreements and users – may need translations and hard-copy signatures.>

This sample agreement and the material contained herein are for informational purposes only, and do not constitute legal advice or legal opinion. You should not act or rely on any information contained herein. BYOD (including wearables) and other employee device programs can vary significantly.