Bring Your Own Device

Individual Liable User Policy Considerations

Good™

Contents

Introduction

As more companies embrace the broad usage of individual liable mobile devices for access to corporate applications and data, Good Technology is often asked for guidance on the establishment of an associated individual liable usage policy. This policy document is intended to provide guidance on questions that companies should ask themselves when establishing their own policies and related considerations.

Policy Document Objectives & Legal Disclaimer

Only your combined Information Technology (IT), Human Resource (HR), Finance, and Legal functions—working closely with your executive team and business unit managers—can determine the exact corporate liable and/or individual liable policy that best fits your company, meets its financial goals and objectives, and takes into account security, legal, regulatory, tax, or other requirements and considerations that may uniquely apply to your Company and its operations.

Accordingly, the objective of this white paper is not to define an actual individual liable user policy. The questions and policy considerations outlined herein are just that, and must not be construed either individually or collectively as: (i) an actual or complete policy; (ii) either necessary or sufficient to meet the fiduciary, legal, regulatory, or other requirements that may apply to a particular company or policy; or (iii) legal or finance advice.

Good Technology disclaims any and all liability for the use of this document and/or the considerations outlined herein, either in whole or in part, in the definition and/or application of specific policies by any company.

Eligibility Considerations

Questions to Ask

- Are all employees eligible for mobile access to company data and applications?
- Will you restrict access, even within the individual liable population, based on role, title, manager approval, geography, or other organizational considerations?
- Will you restrict access for individually liable users to particular company applications or data? If so, which apps and data?
- Will you support any individual liable device, or, for example, only devices explicitly certified by Good Technology for use with Good For Enterprise?

Policy Considerations

- Policy should clearly address:
  - All eligibility requirements
  - Any device support limitations
  - Employee risks and responsibilities
  - Any applications or data access limitations
- Any processes for obtaining approval

Reimbursement Considerations

Questions to Ask

- Are individual liable users ever entitled to reimbursement?
- If so, for which services and under what conditions (e.g., voice usage, data usage, Wi-Fi hotspot usage, roaming usage, business vs. personal usage, manager approval, etc.)?
- Are any services not eligible for reimbursement (e.g., SMS/MMS, ringtone downloads, 411 calls, any service not explicitly identified as eligible for reimbursement)?
- Are there any caps on reimbursement (e.g., in the form of fixed monthly stipends or maximum-expense backlimits, irrespective of charges incurred)?
- Are individual liable users ever eligible for full or partial reimbursement of device acquisition or replacement costs?

Policy Considerations

- Policy should clearly address conditions for reimbursement and eligibility of devices, i.e.:
  - Reimbursement of device purchase and/or replacement costs (e.g., no reimbursement, full, partial up to a limit, frequency of reimbursement, etc.)
  - Any reimbursement limitations (e.g., services, max amounts, etc.)
  - Any monthly stipend amounts and related eligibility

- Maximum reimbursement amounts

- Policy should encourage users to consider voice plans, unlimited data plans, roaming plans, etc. that do not exceed monthly stipend and/or maximum reimbursement amounts. However, policy should clearly state that, should the user choose a plan which exceeds these costs, the company does not assume any financial responsibility, except as otherwise consistent with policy.
  - For example: if stipend amount or reimbursement max is $100/month and user chooses an unlimited voice/data plan with international roaming option at $300/month, policy should clearly state that the company is not liable for the cost difference.

Security Considerations

Questions to Ask

- What is your policy and process for handling a lost or stolen device?
- What is your policy and process for handling the decommissioning of a device (e.g., if user switches to new device, change in user's role/title deems them no longer eligible for access, user leaves or is terminated by company, etc.)?
- Will your company wipe the entire device, corporate data and apps only, or both?
- Will you allow user to initiate wipe action(s) themselves (e.g., through self-service portal)?
- Will your company set and enforce use of a whole device password?
- Will your company ever wipe the whole device?
- Will your company only set and enforce password on the Good client?
- Will your company only wipe data explicitly managed by the Good client?
- Will your company require limits on the use of cameras, browsers, Bluetooth, or other applications and services?
- Will you require users to acquire and install anti-malware as a condition for access to corporate data and apps? Will you provide such anti-malware? Will you require particular vendors or versions?
- What is your policy and process for a user device that has been infected with malware?

Policy Considerations

- Policy should expressly prohibit: (i) device "jailbreaking," "rooting," or the equivalent; and (ii) making any other modifications to device hardware and/or OS software beyond routine installation of updates as directly provided by the applicable device maker or mobile operator. Performing such actions or making such unauthorized modifications is essentially an "inside attack" on device, application, and data security, and should be treated very seriously.
- Policy should be clear on process and timing requirements for reporting lost or stolen devices, changing to a new device, and actions to be taken when an employee leaves the company.
- Policy should be clear on whether or not you will require use of whole device password and associated requirements for frequency of change, minimum strength, etc.

- Policy should be clear on whether or not you will wipe whole device and conditions under which you would do so (e.g., lost or stolen device, change to new device, move to new role, departure from company).
- Policy should clearly state that you always reserve the right to wipe either company data and applications and/or the whole device if deemed necessary in your sole discretion to secure company data or applications.
- Policy should be clear that wiping company data and applications may impact other applications and data (e.g., including but not limited to native Address Book data).
- Policy should disclaim any liability for loss of personal applications or data, whether directly or indirectly resulting from the usage of company apps or data, and/or the wiping of such apps or data, or the whole device.
- User should be encouraged to minimize the risk of losing personal applications and/or data..
- Policy should be clear on any restrictions on the usage of cameras, browsers, Bluetooth, or other applications and services. The ability to enforce such restrictions may be dependent on device capabilities, which in turn may become an eligibility consideration).
- Policy should be clear on any requirements for the use of anti-malware (including specific vendors or versions as applicable) and process and timing requirements for reporting any suspected instances of malware infection.

Acceptable Use Considerations

Questions to Ask

- What is your policy regarding use of device by users other than corporate end-user?
- Will you provide intranet access to individual liable users?
- Will you require individually liable device users to conform to acceptable use guidelines on all Internet usage, even if not enabled through corporate infrastructure and/or for personal reasons (e.g., as a condition of receiving stipend, reimbursement, or access to company apps or data)?

Policy Considerations

- Policy should be clear on whether device enabled for corporate apps and data access may be used or loaned to other users (e.g., if a Good client has a separate password and the whole device password is not used, it may be acceptable for company end-user to allow someone else to temporarily use the device, as use of device does not require company end-user to first “unlock” the Good for Enterprise client that enables access to corporate data or apps).
- If you provide intranet access (e.g., through Good Mobile Access or mobile VPN client), policy should be clear that company’s acceptable use guidelines for desktop/laptop browser usage will apply to any usage of intranet and/or internet access that is enabled through the use of Good Mobile Access or other mobile VPN infrastructure.
- Most companies will not apply acceptable use policies to usage not enabled through corporate infrastructure—if your company chooses to do so (e.g. as condition of receiving stipend or reimbursement), then policy should be clear on this.

End-User Support

Questions to Ask

- Will you provide any end-user support for individual liable users?
- If so, for what applications, services, or scenarios (e.g., lost or stolen device)?

Policy Considerations

- Policy should be clear on what support, if any, will be provided and: (i) explicitly for which applications, services, and scenarios; (ii) any "self-service" actions that must first be taken before requesting support; and (iii) process and/or tools for requesting support (e.g., submitting trouble ticket vs. calling).
- Many companies will opt for individual liable support policy that is expressly limited to the Good client and applications and require that users first attempt to resolve routine issues via "self-service"mechanisms (e.g., always contacting carrier for billing issues, contacting carrier first if not able to connect, resetting own password via self-service portal). This is a key advantage of Good's approach in which the Good client clearly and cleanly separates access to and usage of corporate apps and data from personal apps and data and the rest of the device.

Policy Violations

Questions to Ask

- What should happen if user violates policy?
- Should different violations be treated differently (e.g., eligibility vs. security vs. acceptable use)?

Policy Considerations

- Policy should be clear on consequences of policy violation and any differences from one policy or policy type to the next.

Unauthorized Access or Use of Cellular Telephone Service

On receipt of a monthly bill, enterprise users should immediately check the call detail record section of the bill for any indication of unauthorized calls. Discovery of any such calls should be immediately reported to:

- The carrier providing the service
- The security department

Additional Info: Smartphone Policies & Security

The use of a Smartphone in connection with (Company Name) business is a privilege granted to employees through approval of their management. (Company Name) reserves the right to revoke these privileges in the event that users do not abide by the policies and procedures set forth below.

The following policies are aimed to protect the integrity of (Company Name) data and ensure it remains safe and secure under (Company Name) control. Please note that there may be limited exceptions to these policies owing to device limitations between vendors.

(Define corporate policies here. Note: These are only examples and will vary per enterprise.)

- Your device will lock your account after 10 failed login attempts.
- Your device or Good application will lock every 30 minutes requiring reentry of your password.
- Your device will include password rotation every 90 days.
- The password must be a minimum of six characters.
- The password must contain at least one letter or number (except on devices that cannot accept alphanumeric passwords).
- The password must not be one of your previous four passwords.
- Your device will be remote wiped if: (i) you lose the device; (ii) you terminate employment with (Company Name); (iii) IT detects a data or policy breach or virus; or (iv) if you incorrectly type your password 10 consecutive times.
- Your iPhone, iPad or Android w/ Good device may allow for only the remote wipe of (Company Name) data. This means your personal data is still vulnerable, and thus it is recommended you also set a device password and take additional security precautions.
- In addition to the above security settings, all users are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, “jailbreaking” your iPhone.

Personal Smartphone: A personal Smartphone can be connected to the (Company Name) infrastructure (Good service), but the user is personally liable for the device and carrier service costs. Users of personal Smartphones are not eligible for expense reimbursement for hardware or carrier services. Users of personal Smartphones must agree to all terms and conditions in this policy to be allowed access to those (Company Name) services.

Employees that purchase a device on their own that is not in line with our standard approved device lists may not be allowed to have their devices added to the servers. It is highly recommended that the employee refer to the Smartphone support website to review the devices that are being supported by IT. Users of personal Smartphones are not permitted to connect to (Company Name) infrastructure without documented consent from (Company Name) IT. Furthermore, (Company Name) and (Company Name) IT reserve the right to disable or disconnect some or all services without prior notification.

Release of Liability and Disclaimer to Users of Personal Smartphones Users (Company Name) hereby acknowledge that the use of a personal Smartphone in connection with (Company Name) business carries specific risks for which you, as the user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which could render a device inoperable.

(Company Name) hereby disclaims liability for the loss of any such data and/or for service interruptions. (Company Name) expressly reserves the right to wipe the Good application (or similar applications) at any time as deemed necessary for purposes of protecting or maintaining the (Company Name) service.

Furthermore, depending on the applicable data plan, the software may increase applicable rates. You are responsible for confirming any impact on rates as a result of the use of: (Company Name) - supplied applications as you will not be reimbursed by (Company Name). Finally, (Company Name) reserves the right, at its own discretion, to remove any (Company Name) - supplied applications from your Smartphone as a result of an actual or deemed violation of the (Company Name) Smartphone Policy.

See for yourself how Good can improve mobility for your organization. Visit http://good.com/trygood.

Good Technology
For more information,
please call 866 7 BE GOOD
or visit www.good.com.

Global Headquarters
+1 408 212 7500 (main)
+1 866 7 BE GOOD (sales)

EMEA Headquarters
+44 (0) 20 7845 5300

BYOD_Policy_Jan2012_US