USE OF PERSONAL MOBILE DEVICE TO ACCESS COMPANY INFORMATION POLICY

Quick summary: This policy applies to personal mobile devices used to access company or client information and governs the use of such devices for Accumen and client-related business purposes.

Audience: ALL

Responsible Dept.: Compliance	**Owner:** Security Officer
Initial Policy Approved Date: 11-20-14	**Current Version Approved Date:** 11-20-14

Policy Statement and Purpose

Accumen Inc., a Delaware Corporation ("Accumen") permits you as an employee to use your own personal mobile devices, including tablets, smartphones, and handheld computers ("device(s)") for legitimate Accumen-related business purposes. To protect Accumen and its employees, however, your use of a device for business purposes must conform to this policy. You are responsible for using your device in a sensible, ethical and lawful manner. Violation of this policy may be grounds for disciplinary action up to and including termination of your employment. Nothing contained in this policy is intended to restrict communications or actions protected or required by state or federal law. For any questions relating to this policy please contact your manager or the Compliance Department.

Scope

This policy is applicable to any and all Accumen employees who elect to use mobile electronic devices to access Accumen or client information, regardless of employee location.

Table of Contents

Definitions

The below definitions apply to this policy:

- Device(s): Employee's personal mobile and handheld devices, including tablets and smartphones.
- Jailbreak: Installing software that allows the user to bypass standard built-in security features and controls

Policy and Procedures

1. No Expectation of Privacy. You should have no expectation of privacy in any content created, received, transmitted, printed, stored or recorded on or from your personal device to the extent such content relates to Accumen's business, contains Accumen information, or is generated using Accumen-hosted tools (e.g., email or company-supported applications). Accumen reserves the right, without notice, to monitor, intercept, review, store, and erase any such content on your personal device. This may include, without limitation, the monitoring, retrieving, recording, and disclosing of your communications, content or other applicable information from your device, whether or not the device is in your possession.

   With exception of the preceding paragraph, Accumen will respect the privacy of your personal device and your personal information contained on your device and will only request access to your device to implement security controls, as outlined below, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings involving Accumen. Accumen will not monitor your personal: emails, text messages, photos, calendars, call logs, voicemails, or other application data or personal information stored on your device. This policy differs from the Accumen-provided equipment or services (such as your company-issued laptop) policy, where you do not have a right or expectation of privacy. You may elect not to use your personal device for business purposes and, if you believe a device is required to perform your work function, you should discuss with your manager and, if appropriate, Accumen will provide you with a reasonable company-owned device.

2. Confidential Information. Accumen's confidential information and intellectual property, and that of its clients, are extremely valuable to Accumen and its clients. You must not jeopardize such information through misuse of your device. Unauthorized disclosure of Accumen's confidential information or intellectual property (or that of its clients) to anyone outside of Accumen is strictly prohibited. All Accumen work product (or that of its clients) created, stored or maintained on your device is subject to the confidentiality and proprietary interests obligations between you and Accumen.

3. Requirements for Accessing Accumen Network Services from your Personal Device.

   - You are required to password protect your device(s) and comply with all Accumen password policies as issued, including use of strong passwords.

   - You must immediately report to Accumen any device used under this policy that is lost, stolen, retired, accessed by unauthorized persons or otherwise compromised, so Accumen can assess the risk and, if necessary, remotely erase the content on the device, or select portions thereof containing Accumen data (to the extent practicable).

- You agree to comply with Accumen's device configuration requirements and not alter the security settings of the device without Accumen's consent.

- You agree to set your device(s) to logout or lock out after not more than 10 minutes of inactivity.

- You agree to maintain your original device operating system and keep your device current with security patches and updates, as released by the manufacturer.

- You will not "Jail Break" the device (installing software that allows the user to bypass standard built-in security features and controls).

- You agree to delete when appropriate all company or client-related content on your personal device. Follow the premise, "When in Doubt, Delete it Out."

- If you discontinue use of your device under this policy or leave Accumen's employ, you must allow Accumen to: (a) remove any of Accumen's work product or sensitive business content from your devices and (b) disable any software or services provided by Accumen on your devices.

- You give Accumen permission to install and configure security software and consent to Accumen's efforts to manage the device and secure its data, including providing Accumen with any necessary passwords.

- You must provide Accumen with prompt access to your device when requested or required for Accumen's legitimate business purposes, including in the event of any security incident or investigation.

- You must install an application on your device that will be provided by Accumen and will enable the company to perform a "corporate wipe" (removal of Accumen e-mail, data, and any Accumen-provided applications) on your device if your device is lost, stolen, compromised or as otherwise determined appropriate by Accumen (e.g., an exceeded number of failed password attempts on your device that implies a potential security threat). While Accumen cannot guarantee you, it will attempt to the extent practicable, to only delete Accumen-related content on your lost, stolen or otherwise compromised device. You understand Accumen reserves the right to erase completely your device(s), if appropriate, which may result in the loss of any personal information on your device(s) (e.g. contacts, photos, music).

- ❖ You agree to use your best efforts to physically secure your device against loss or theft and prohibit access to any Accumen information by persons who have not been authorized to access the device by Accumen.

- ❖ You agree to not back up any Accumen information on your device to any cloud-based storage or services without Accumen's consent. Any such backups inadvertently created must be deleted and disabled. To the extent you create backups with Accumen's consent, you must provide Accumen with access to your local or cloud-based storage to access and review any such backups when requested or required for Accumen's legitimate business purposes, including in the event of any security incident or investigation.

- ❖ You must also never co-mingle with Accumen information any information developed or obtained during your previous employment engagements.

4. Reimbursement. For reimbursement of any applicable device, please refer to the Accumen Employee Business Expense Policy (Doc 001b).

Acknowledgment of Compliance

Acknowledgment of Compliance

I acknowledge I received and read a copy of the Accumen's Use of Personal Mobile Device to Access Company Information Policy and understand it is my responsibility to be familiar with and abide by its terms. I understand Accumen may modify this policy from time to time and it is my responsibility to review the policy periodically to confirm I am in compliance. This policy does not set terms or conditions of employment or create an employment contract. I understand Accumen has the maximum discretion permitted by law to interpret, administer, change, modify or delete this policy at any time with or without notice. No statement or representation by a supervisor or manager or any other employee, whether oral or written, can supplement or modify this policy. I also understand any delay or failure by Accumen to enforce any work policy or rule will not constitute a waiver of Accumen's right to do so in the future.

Forms	None.
References and Related Documents	Accumen Employee Business Expense Policy (Doc 001b)
Date of Next Review	November 2015
Tags	Compliance; Information Technology; Mobile Device; Confidential Information