The following is a template designed to assist in the policy development governing the protection of company computer systems and assets. As with all templates, this document provides a basic framework for the broad topics for consideration. Footnotes provide prompts for other general considerations and points for discussion. Each organization has unique risks and considerations that necessarily require customization. For more information, contact Ron Raether at (949) 622-2722 or ron.raether@troutman.com, or Mark Mao at (415) 477-5717 or mark.mao@troutman.com.

MOBILE COMPUTING POLICY
Template

Title: Mobile Computing Policy	**Doc. No.** Insert
Issued by: (e.g., Corporate Compliance)	**Original Effective Date:** Insert Month/Year
Approved by: (e.g., Board of Directors)	**Last Review/Approval Date:** Insert Month/Year
Replaces: Insert	**Effective Date:** Insert Month/Year
Cross-referenced Policies: Insert	

PURPOSE

The purpose of this policy is to define guidelines for laptop/mobile computing device safety and security.

APPLICABILITY

This policy applies to all employees, administrative consultants, contractors, temporary personnel, and the like who have been permitted access to Company Sensitive Information or Personally Identifiable Information ("PII")[1] in the Insert Company Name ("Company") network via a laptop computer or other pervasive/mobile computing device, tablet, iPad, iTouch, iPhone, Palm, Blackberry, WebOS, Android, netbook, web-enabled cellphone, and like devices ("Device").

SCOPE

Protection of Devices, especially when used off-site, is necessary in order to reduce the risk of both unauthorized access to the data contained on the Device, as well as the data that the Device has access to on the Company network. Protection is also necessary to safeguard against loss or damage of the Device itself.

[1] As with all privacy and security policies, the Company should clearly define its protected information sets. Whether information is protected may be defined by law, policy, or best practice.

Generally, a Device should be given the same level of protection as Company Sensitive Information and PII in hard copy, on the Company network, or in other Company-controlled environments.

POLICY

This section establishes guidelines, where technically feasible, governing the secure and safe use of Devices.

1. Shipments of new or unassigned Devices are to be stored, within a reasonable time of receipt, in locked closets or rooms with controlled access and no false ceilings or partial walls.

2. Security instructions to users should be included with Device checkout.

3. A locking cable to secure the Device to a large stationary object, such as a desk or airplane seat, will be issued upon request or as needed with each Device, except smartphones.

4. In "open" access areas, a laptop restraint/lockdown device will be used when the computer is left unattended if deemed necessary to protect it.

5. Tamper-proof identification labels with the Company name/ID shall be visibly placed on all laptops to assist in identification if stolen or misplaced. Please note that where a safety issue is involved, the local security environment may necessitate masking the Company name.

6. The Device make, model, serial number, and media access control address is to be recorded and stored in a safe location to give precise information to authorities in case of theft.

7. The Information Technology Department ("Information Technology') is responsible for assuring that all Devices owned by the Company have the most recent software and hardware configuration and available upgrades installed.

8. Unattended storage standards for Devices should be the same as those for the storage of similar hard copy information.

9. Back-ups of Company data onto Company servers should be accomplished on a basis which ensures their availability and negates the significant loss of such data.

10. The user has overall responsibility for the confidentiality, integrity, availability, and accessibility of his/her assigned Company device, and the data on or accessible through the Device.

11. Encryption to maintain confidentiality and protect against the bypass of software controls (*e.g.*, booting from a system disk or USB, file encryption) must be utilized. Encryption will be used when sending and receiving Company Sensitive Information or PII.

12. Anti-virus/anti-malware software will be installed on the Device and all incoming disks/magnetic/digital media /jump drives should be virus-checked before being used.

13. Users must take steps to prevent casual overview or attempted use by unauthorized personnel. The use of privacy screens is encouraged.

14. User ID and authentication is required before access is given to data and applications residing on the Device. Some smartphones only allow for pattern or PIN for authentication without a User ID, which is acceptable for accessing the Device itself.

15. Users are responsible for taking reasonable precautions to protect and maintain Devices. Evidence of misuse or abuse of a Device may result in the revocation of the user's use of such Device.

16. A screensaver and password or "clear and lock" feature will be used to protect the Device if the user must leave the activated Device; a user password must be re-entered for further access.

17. Passwords must meet the standards set forth in the Company's User Authentication IDs and Passwords Policy.

18. To help prevent damage and theft, a laptop should not be placed in or as checked baggage. If a laptop must be left in an automobile, it must be stored in the trunk or otherwise out of plain view.

19. Losses are to be immediately reported to appropriate authorities, Loss Prevention and Information Security.

COMPLIANCE

Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. We reserve the right to advise appropriate authorities of any violation of law.

ACCOUNTABILITY

The Internal Audit Department is responsible for ensuring compliance with the Mobile Computing Policy and the controls created to safeguard the Company and its assets.

EXCEPTIONS

Any exceptions must be approved by Information Security.