calero mdsl

WHITE PAPER

Creating and Maintaining a Strong Mobile Device Policy

www.caleromdsl.com

TABLE OF Contents

You've left something out! Something so important to your mobile device initiative that you would be best advised not to allow anyone to use any smartphone, tablet, or laptop until you've taken care of it.

It's your Mobile Device Policy, a document that defines everyone's rights, responsibilities, and accountability when using any mobile device on behalf of your company. It's every bit as important as the devices themselves, the communication services they connect to, or the continued success of your business.

Purpose/Value of Mobile Computing and Communications to the Business

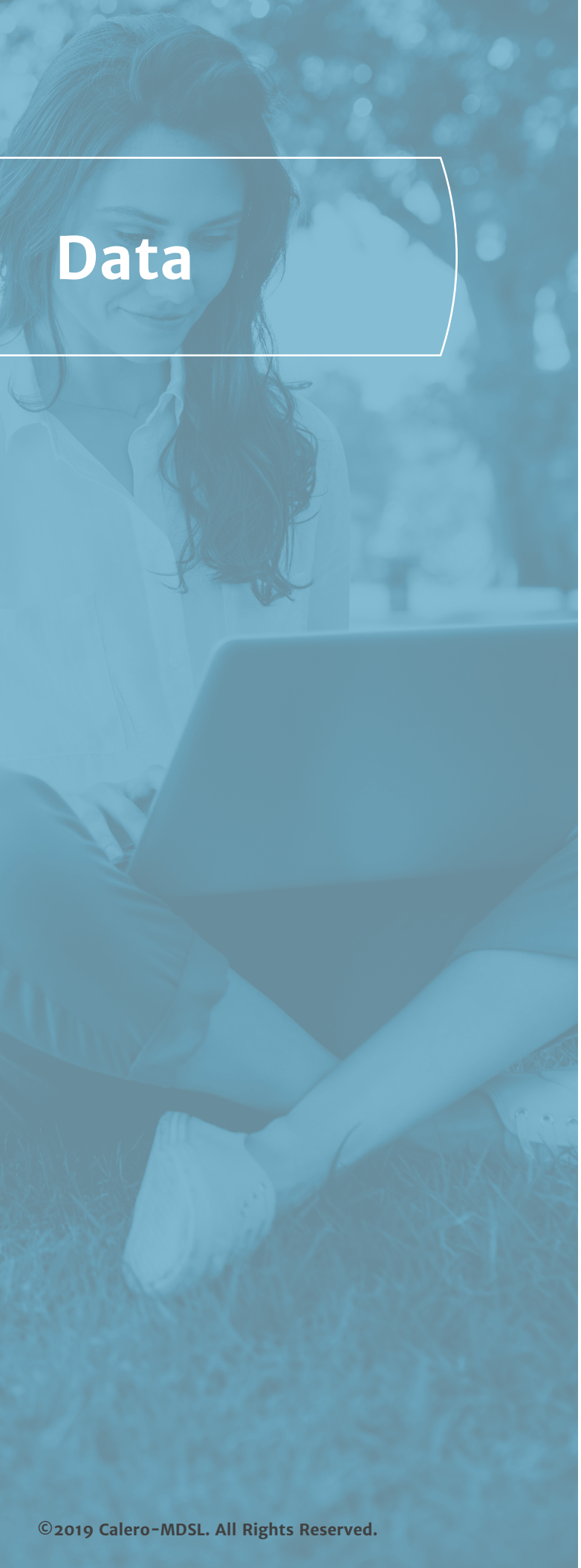
Your Mobile Device Policy provides important protections not only from technical failure, but also from the financial risks of significant overspending, as well as liability and other legal exposures that may arise from the actions of any of your users.

Users are perhaps the most vulnerable of the components in your mobile network. While digital devices and software are consistent in how they'll operate and respond, people are not. While it's unreasonable to expect you can control them as you do digital devices, your Mobile Device Policy fully informs them as to what is expected of them, and what they can expect from you.

The title of this paper talks not only about creating your policy, but also maintaining it. In one respect this refers to the fact that technology and business rules are constantly changing, so this policy is a living document which must constantly be adapted to allow for those changes.

But perhaps the most important definition of "maintaining" as used here is enforcement. Like all policies, your Mobile Device Policy is only as good as how well it is enforced.

"Users are perhaps the most vulnerable of the components in your mobile network."



Data

It's really all about the data. Storing the data. Moving the data. Using the data. That's why we use mobile and on-premise equipment to begin with; to manage and secure the data while its resting in storage and while its being transported from device to device.

Especially for companies that have instituted a "bring-your-own-device" (BYOD) policy, there is need to keep data in its proper place. That is, the data your company owns must be forever segregated from the personal data owned by the user. This segregation must prevent the user from sharing corporate-owned data using their own personal email, messaging, or other data communications software. Failure to do so renders literally all corporate data security measures completely useless as it provides an open doorway to unauthorized access.

Most companies that are allowing users to access their network with personally owned devices are using container technology through a Mobile Device Management (MDM) application to keep corporate and personal data separated.

Choice of Devices

The first set of decisions which must be made actively centers on which devices to allow onto your network. Some companies strive to furnish a long list of acceptable devices to accommodate as many users as possible. They soon find that the mere maintenance of this catalog becomes overwhelming. Devices are constantly being updated and replaced with new versions, with normal product lifecycles running from 9 to 24 months. Needs are also constantly changing. Your device policy must have enough agility to readily adapt. And, your mobile procurement portal must have the business logic and task automation to enforce approvals based on the user making the request.

There are several categories of considerations which must be taken into account when deciding which and how many devices to approve:

Functional

Like any computing device, mobile devices run an operating system to enable all applications and features. That operating system must be compatible with those operating in your network environment. They must also be manageable and securable by your IT team.

Any mobile device approved for use on your network must possess the functionality required for the user to perform required tasks and functions. Workers operating in hazardous areas may require ruggedized equipment to withstand those demands. Those performing highly analytical functions may require faster processors, or more memory. Salespeople whose devices will constantly be seen by customers may require the device to be aesthetically pleasing in appearance.

Your device policy must have enough agility to readily adapt.

> A compromise must be achieved to balance support cost against user agility.

Hierarchical

Intuitively, one would surmise that the more important the user the more sophisticated the device. In many environments, however, this is not the case. Instead a hierarchy of needs is established. "Power-users" who perform important, complex tasks are assigned more powerful, more feature-rich devices. Productivity and Information Workers may receive midrange units. Senior executives whose mobile use may only extend to email, voice, and perhaps video communications may use far more fundamental models since they don't require the horsepower.

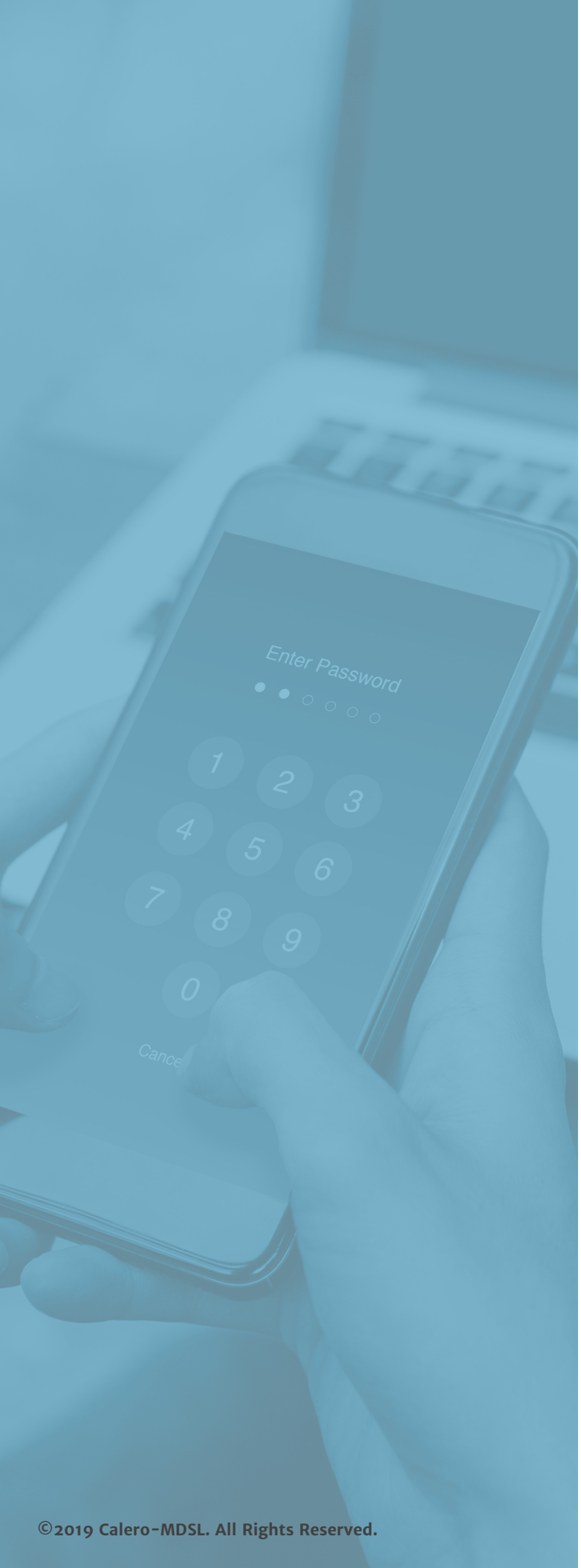
Financial

An obvious consideration must be the total cost of ownership (TCO) and operation of the device. As new generations are introduced such as the upcoming arrival of much faster 5G service, the price of each device and its service skyrockets. Companies may be able to mitigate this as carriers offer programs to reduce the impact of device price on budgets. TCO extends beyond differences is purchase price to include all costs required to maintain and operate the device for its entire produce lifecycle.

Support

Lacking controls, some companies have found their IT support department confronted with the need to support hundreds or thousands of devices each running different combinations of operating systems, applications, utilities, security products, and more. Each support event becomes an expensive and time consuming adventure as IT personnel seek the tools and resources needed to provide the required help.

When an environment has only one permitted configuration of one approved device, support becomes about as simple and inexpensive as can be imagined. Each additional device or configuration adds complexity and therefore cost. A compromise must be achieved to balance support cost against user agility.



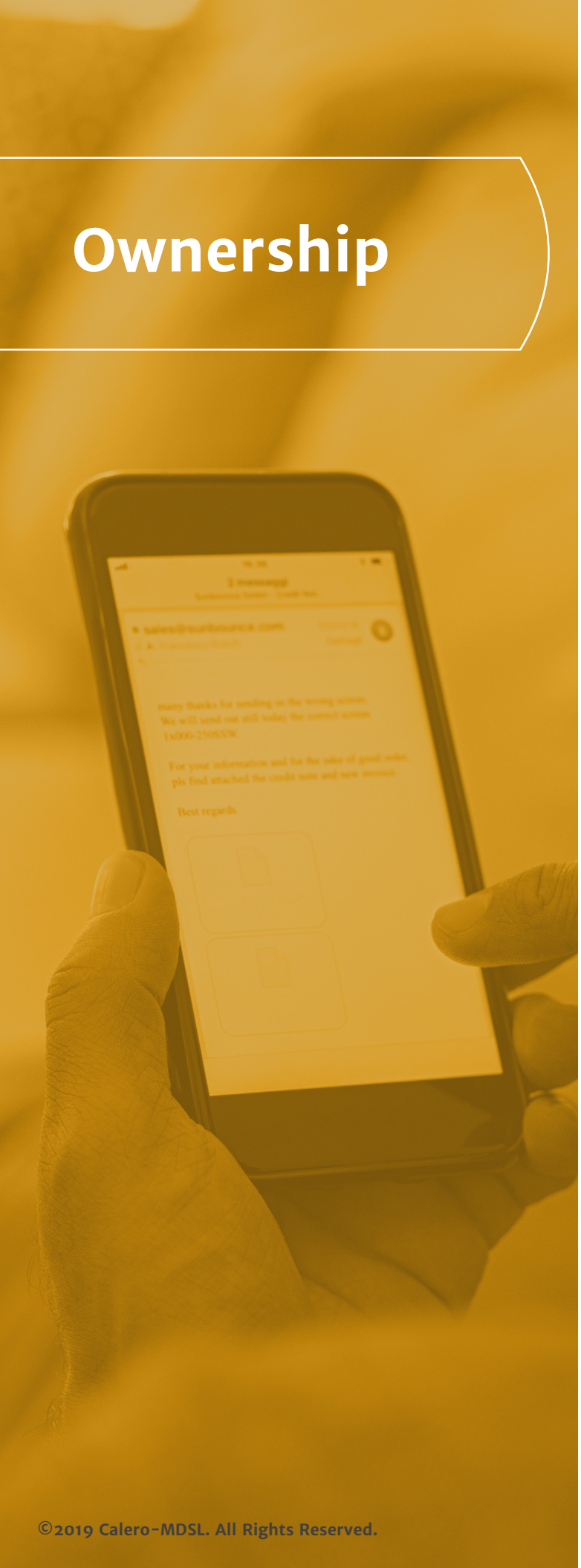
Security

Another balance which must be achieved is between the users' desire for maximum ease-of-operation of their device against the corporation's need to keep all data and devices secure from unauthorized access. Users want fewer required passwords. The corporation requires multi-factor authentication. The middle ground is not always apparent, but is by necessity achievable.

Ideally, a specific device should be offered at each level of user sophistication. An entry-level device for productivity workers and executives. A mid-range device for those producing more volume or other work requiring more horsepower. And, finally, a power-user device to support the most sophisticated analytical information workers. Some companies are allowing one in each category running the Android operating system, and another running the Apple iOS operating system for iPhones and iPads.

For every rule there are often exceptions. Even these must be carefully defined in your policy. How many levels of approval must be obtained to allow devices other than those specified by the company to join the corporate network? That may be conditioned on level of user, criticality, or other factors.

Ownership



Device ownership is also a key consideration. Where the company had always owned all computing equipment provided to all users, more recently there has been a rise in the users' desire to use the same comfortable, familiar device to live, work, and play. Not only is the ownership of the device a consideration, so is the price paid monthly for access services, and who pays it.

This creates a simple decision table containing the following questions:

Who owns the device?

Although BYOD initiatives brought the promise of more freedom and flexibility for employees, and more work contribution from them for management, the reality is that users were very hesitant to give their company control of their personal device. Choose-your-own device (CYOD) has gained in popularity as users go back to carrying two devices.

In cases where the employee owns the device, the company may want to specify how often it must be upgraded, and how often it must be replaced with a newer model to accommodate new security and other operating specifications. The company may also establish requirements specific to the user's role, such as ruggedized casing for employees working in hazardous environments, or minimum processor, clock speed, and storage for "power-users." Consider also requiring the user/owner to keep all operating software constantly up to date, use a secure password and PIN, routinely backup the data on the device, and always keep all data.

In cases where the company owns the device but allows personal use, they may want to forbid the user to add apps, or specific apps, or paid apps, or apps not appearing on an "approved apps" list to the unit. Users should also be required to confirm that they will report immediately should a device be lost or stolen.

Who pays for the access services?

A company paying for hundreds or thousands of users will doubtlessly qualify for deeper discounts from carriers, but then carry the cost of managing all those accounts. This encourages some to provide their employees with a stipend for their carrier services payment. In other cases, carrier services may be completely the responsibility of the employee.

If the company is allowing use of personally-owned devices, they should establish specific access service requirements, such as regional, national, or international roaming and other features. These may require the user to engage the services of specific carriers.

What may the device be used for? Business use only? Personal use? Both?

This is not necessarily a binary decision. If the company decides to accommodate employees by allowing personal use of company-owned mobile devices, they may establish specific rules for what can and what cannot be done on the device. Forbidding the sending of emails containing attachments, for example, will discourage one of the biggest dangers to corporate data, that they could be attached to personal email and sent to unauthorized persons. Many such guidelines may be established to limit personal use to specific non-business times of day or messages under a certain size. These should all be part of a more encompassing Acceptable Use Policy (AUP).

Whose phone number is on the device?

Recently, as phone numbers have become more portable, many users prefer to have a phone number they've had for years on their phone. Companies are accommodating this in growing number. Users are also permitted to take their phone number with them when they leave.

Expectation of Privacy

Regardless of device or service ownership, all users must be advised that your network is a corporate-owned resource and, as such, they can have no expectation of the privacy of anything that passes through it. Also, their use of the company's email server requires them to observe acceptable use policies in the formation of messages of any kind. If they are not so notified, you may be liable for any inappropriate communication they initiate.

Device and Data Security

In order to protect the corporation, all users must be clearly advised to never overcome any data or network security measures implemented by the company, and that all corporate data remains the property of the organization. This preserves specific rights for the company.

The company may elect to periodically scan each device to determine if any undesirable changes have been made to it. Depending upon ownership of the device, they may require adjustments to be made, or have the device removed from network access.

It is also advisable to establish malware detection and also detection of "jailbroken" Apple iOS or "rooted" Android devices which give mobile device users far greater access than they should have. At all times the company must reserve the ability to completely or selectively erase device contents in event of possible loss, theft, or compromise. Provisions must also be made, either in the remote erasure strategy or the corporate user policy, to deal with indemnification of responsibility for personal data lost during such erasure.

Failure to Offboard

Perhaps the most common policy error is the failure on the part of so many companies to properly and completely offboard departing employees from their network. Incorporating an employee agreement to not access the company network after departure from the company provides at least a legal protection against this exposure, but only an automated, routinized process provides greater assurance that access has been terminated.

Perhaps the most common policy error is the failure on the part of so many companies to properly and completely offboard departing employees from their network.

Confirmation

Finally, it is critical to maintain documentation that all employees have read and understand the policy. Signing and dating a statement to that effect provides the final level of assurance that each user considers the entire policy altogether enforceable, which should serve as an adequate deterrent to those considering violation.

Remember that contracts such as your Mobile Device Management policy are written during the best of times to allow for proper behavior at the worst of times.

Enterprises are best served by working with a knowledgeable vendor who can help you protect your data, your network, your users, and your assets with a comprehensive mobile device management policy.

calero mdsl

For more information about Calero-MDSL,
please contact us:

+1.866.769.5992

info@caleromdsl.com