



Mobile Device Policy and Program

General Policy

This policy provides standards and rules of behavior for the use of mobile devices and/or tablets provided by DECISIONONE Corporation (“D1”)(“Mobile Device(s)”) to access D1 systems, information and/or services. This policy applies to employees, contractors, consultants, temporaries, and other workers at D1, including all personnel affiliated with third parties (“Mobile User”) who have been provided with a Mobile Device by D1 and work in D1’s North American Business Units and/or whose primary office is located within North America (“Mobile User”).

Each Mobile User reads, accepts and will abide by the provisions set forth herein. At D1’s sole discretion and expense, Mobile Devices (and telecom carrier services) are being entrusted to specific employees with a business need for that device. Eligibility for this Mobile Device Program is based on job roles and responsibilities. D1 reserves the right to make any determinations concerning each Mobile User’s need for a Mobile Device. This Mobile Device Policy outlines acceptable use, reimbursements and other administrative issues relating to the Mobile Device Program.

Protecting the security and integrity of D1 and our customers’ data and technology infrastructure is of the utmost importance.

Mobile Devices are the property of D1 and the Mobile User is responsible for using it appropriately, minimizing wear and tear, as well as keeping the Mobile Device safe and secure from potential theft or loss.

This policy shall:

- Support employees’ job duties with mobile communications
- Promote employee safety when using mobile communications
- Limit corporate liability
- Improve management of mobility costs, and
- Maintain corporate data security and network security.

Safety

All Mobile Users must obey all local traffic laws and use common sense when operating a motor vehicle. D1 has a zero-tolerance policy for texting or emailing while driving. No text, email or communication is worth jeopardizing your physical safety or the safety of others around you.

When dialing a number, or using the keypad, all Mobile Users should come to a complete stop, pull out of traffic to the side of the road, and/or pull into a parking space. Mobile Users are encouraged to use voice-activated calling or pre-programmed numbers, provided it does not distract from safe driving.

Hands-Free communication is the only acceptable method of Mobile Device use while operating a motor vehicle. Any other Mobile Device activity that prevents a Mobile User from focusing on driving such as surfing the web, texting, emailing, using applications, or other activities, is strictly prohibited.

Mobile Device Data

By signing this Policy below and by using the Mobile Device, each Mobile User consents to D1 periodic monitoring, reviewing and accessing data usage, telephone numbers and other data contained on the Mobile Device.



In addition, D1 reserves the right to remotely wipe all data from that Mobile Device. Instances where a remote wipe may occur include, but are not limited to: reports of a lost, stolen or misplaced Mobile Device, suspension or termination of employment. Mobile Users are not permitted to store data on remote memory cards.

D1 is not responsible for accidental deletion of personal data on devices that connect to corporate e-mail.

Data Usage

Each Mobile Device is set with a specific monthly data plan ("Plan"). The Plan resets with each billing cycle. Mobile Users will make every effort to adhere to the Plan and compliance will be measured by comparing a Mobile Users actual usage to allowable usage limits under the Plan. Sending and receiving e-mail, photographs, web browsing, GPS and software applications all use data.

Initial Plan overages will result in a warning. A second overage will lead to notification to the Mobile User's manager and commensurate remedial action. Persistent Plan overages may lead to revocation of Mobile Device use or disciplinary action. If any such overages are attributed to excessive personal use, D1 reserves the right, with written notification, to deduct those monthly Plan overage charges from the employee's pay.

Self-monitoring of data usage is available on each Mobile Device. Typically, this feature is located in 'Settings'. If you are unable to locate this feature, please contact the IT Department.

Acceptable Use

At no time should Mobile Devices be used to:

- Store or transmit illicit materials
- Harass others
- Engage in outside business activities
- Conduct illegal business
- Engage in obscene behavior

Mobile Users should use secure Wi-Fi networks at corporate locations. Mobile Users should never use public networks.

Mobile Users may use Mobile Devices to access their email, calendar, contacts, documents and D1's systems.

Inappropriate websites are blocked through our IT policy management protocols. If you are unsure, refer to D1's Code of Conduct and refrain from accessing unknown websites on your Mobile Device. Mobile Users should refrain from accessing Facebook or sports websites on their Mobile Devices; as these sites, may expose Mobile Devices to viruses and malware.

Mobile Users are permitted to use Mobile Devices for limited personal use. However, data usage and charges associated with using Mobile Device for personal communications, including text messages, email and voice calling, will count towards the monthly Plan limits. Therefore, personal use of Mobile Devices should be minimized.

All Mobile Users must adhere to all federal, state and local laws and regulations regarding the use, transmission of data, images and accessing certain sites on Mobile Devices. Users discovered to be in violation of this Acceptable Use provision of this Policy may be subject to disciplinary action, up to and including termination.



Expense Reporting and Reimbursement

This Mobile Device Program replaces any previous mobile phone reimbursement and stipends processed through the D1’s Travel and Expense (“T&E”) system. Any users who are not eligible for this Mobile Device Program may continue to process mobile phone expenditures utilizing the T&E system, with prior approval by their manager or supervisor. Expenditures processed through the T&E system must be reasonable and will be monitored.

Porting of Mobile Phone Numbers

D1 will not transfer (“Port”) personal mobile phone numbers to a Mobile Device. D1 will not Port existing D1 mobile phone numbers between wireless carriers, nor will it Port D1 mobile phone numbers to personal mobile phones.

Any exceptions will be considered on a case-by-case basis. For example, if changing a mobile phone number would negatively impact D1’s customers or relationships. Any phone number Ported to D1’s Mobile Device will become D1 property.

Policy Administration

The Office of the CIO will ensure compliance with the provisions listed in this Policy and Program and administer it in accordance with the guidelines as set forth herein. This Policy may be modified from time to time. With prior written approval by the IT Department, limited exceptions to the policy may occur due to variations in devices, platforms and business needs.

If any portion of this Policy is declared void, nonbinding or otherwise unenforceable, such portion shall be considered independent and severable from the remainder of this Policy, which shall remain valid and unaffected.

By signing below, I am indicating that I have read, reviewed and acknowledge acceptance of the provisions of this *Mobile Device Policy and Program*.

MOBILE USER SIGNATURE

DATE

MOBILE USER PRINTED NAME

JOB TITLE