Document ID:	V2SOFT_Mobile_Device_Telework_POLICY
Document Name:	Mobile Device Policy
Version #:	1.1
Author:	Shankara Narayan

Reviewers:	Muktish	**Date:** 16-Jan-2017
Approvers:	Manjunath	**Date:** 16-Jan-2017

Revision History

Version	Update Date	Author	Description	Reviewed By	Approved By
1.0	8-Oct-2015	Shankar a Narayan	Initial Version	D. S. Srinivas	D. S. Srinivas
1.1	16-Jan-2017	Shankar a Narayan	Updates to Section	Muktish	Manjunath

Table of Contents

1 Introduction

V2soft Pvt. Ltd. provides a wide range of Technology and Consulting Services including IT Services, Cloud Computing, Engineering Solutions, Mobility Solutions, Big Data Analytics, Testing Solutions, Hosting Solutions and Staffing Solutions to clients in the healthcare domain. This is a statement of commitment to protect the personal health care information in compliance with the HIPAA and data protection legislation.

We have established V2Soft Management System Framework for setting Process and Objectives for Information security and Healthcare data protection on a Risk based approach with Business Owners of Healthcare groups as HIPAA Risk Owners for complying with the HIPAA and data protection legislation.

V2Soft recognises that to ensure the most effective running of services, communications and business activities it is necessary for some employees to have access to mobile and data dongle communication devices. These guidelines and related procedures should be applied consistently to ensure the correct use of V2Soft assets in relation to procurement, maintenance and payment for these facilities.

The Mobile and data dongle device Policy should be complied in conjunction with other Information Security Policy and Data Protection Policy of V2soft Pvt. Ltd.

1.1 Acronym/Abbreviation and Definitions

Acronyms	Expansion
Basic Smart mobile phone	Blackberry with physical keyboard.
Advanced Smart mobile phone	A smart phone such as a touch screen Blackberry, Android, Apple iPhone or Windows phone. Current models.
BYOD (Bring Your Own Device)	A personally owned device where permission to use a V2Soft supplied contract SIM has been given or a personally owned device with a personally paid airtime contract.
Data Dongle	Device that adds 3G/4G connectivity to a laptop computer or similar device.

Data Tethering	Where a mobile phone is utilised to enable 3/4G data connection to a Laptop instead of a Data Dongle.
Mobile Device	A mobile phone handset, data dongle, SIM or tablet computer, including iPads.
Mobile Phone	A mobile handset for data and/or voice & text messaging.
Tablet	Apple iPad, Android, Windows based tablet or
ISM	Information Security Manager
CISO	Chief Information Security Officer
HIPAA	Health Insurance Portability and Accountability Act
OPAL	Organization Process Asset Library
COM	Common
EDS	Electronic devices
BCP	Business Continuity plan

1.2 Scope

This Policy & Objectives are applicable to all Employees, Consultants, Suppliers, all interested parties & all Stakeholders.

The Policy is Approved and Mandated by the Management of V2Soft Pvt. Ltd.

1.3 Purpose & Guidelines

To establish the expectations and responsibilities placed on all V2Soft mobile and Data card device users with authority for the acquisition and/or use of devices, tariffs or licences procured in respect of the provision of mobile communications options necessary for the V2Soft to meet its corporate responsibilities and business needs.

2 Mobile Device and Teleworking Policy

V2soft Pvt. Ltd is committed to implementing security measures to manage the risks introduced by using mobile devices.

Where a mobile phone and Internet Dongle has been issued by the company, it is for business use only and always will remain the property of the Company. The user(s) will be responsible for its safekeeping, proper use, condition and eventual return to the Company. The user will also be responsible for any cost of repair or replacement other than fair wear and tear.

A mobile phone is provided primarily to enable the user to do their job, i.e. to keep the Company informed at the earliest opportunity of matters which it needs to know about and to be similarly contactable by the Company, or to contact customer/client when working away from Office. Therefore, it is the user’s responsibility to ensure that the mobile phone is kept charged and switched ON always.

Users should not sign up to text based information services, e.g. SMS alerts from SHOPs, text voting etc. The use of the internet on Company Mobile Phones is strictly prohibited, except in the case where specific authorisation has been given by the Director or respective supervisor.

Unless agreed by the Director or respective supervisor, applications and other programmes may not be downloaded to any mobile phone under any circumstance.

The SIM card from Company mobiles should not be placed into any other mobile, unless to another Company issued mobile phone. Neither should the camera facility be used for anything other than an emergency, e.g. company car accident where evidence may be required.

The Company recognises that users may, on occasion, have to make personal calls or send personal text messages during working hours, or outside normal working hours. Where it is deemed that an unreasonable amount of personal calls/text messages have been made using the mobile phone, the Company reserves the right to deduct those costs, either through deduction from pay, or otherwise. The Company may, after formal investigation, take action under the Disciplinary Procedure if such use is excessive or unauthorised. Users will be expected to make payment for private calls made beyond reasonable usage.

If it is found, following investigation, that there has been excessive personal data use, then the user will be asked to reimburse the company for the cost of this and action may be taken under the Disciplinary Procedure.

The user agrees that upon termination of employment, should they not return the allocated mobile phone, or should the mobile phone be returned in an unsatisfactory condition, the cost of replacement, or a proportional amount of this as decided by the Company, will be deducted from settlement, or the user will otherwise reimburse to the Company.

3 Mobile Device and Teleworking- Objectives

1) To put in place safeguards to protect to ensure the security of teleworking and use of mobile devices.
2) To ensure that business information is not compromised.
3) To ensure that the mobile devices are used only to accomplish the intended business purpose.

4 Mobile Device Usage

Telework (also known as telecommuting), which is the ability for an V2Soft Pvt Ltd. employees and contractors to conduct work from locations other than the organization’s facilities.

Teleworkers use various devices, such as desktop and laptop computers, cell phones, and personal digital assistants (PDA), to read and send email, access Web sites, review and edit documents, and perform many other tasks.

Teleworkers may use remote access, which is the ability of an organization’s users to access its non-public computing resources from locations other than the organization’s facilities. The options for providing remote access may include virtual private networks, remote system control, and individual application access (e.g., Web-based email).

All users must adopt practices of fair and reasonable use. Calls should be limited to that for effective business use and kept as brief as possible. The user should take all reasonable and practical precautions to keep the device safe from damage, loss or theft. The user must not use the device for unlawful activities, commercial purposes unrelated to V2Soft, or for personal gain. Use of premium services or chargeable downloads such as third party software, ring tone services, TV or film downloads, competitions or adult chat lines for personal use are strictly forbidden. As with any V2Soft equipment misuse of the mobile device is a disciplinary offence.

When a mobile device or data dongle has been authorised to be assigned to an employee, the following conditions will also apply:

a) The mobile device should, when required, maximise the functionality offered by the V2Soft’s e-Communications infrastructure, email, calendar, and other apps facilities as they become available e.g. remote tracking and resetting (data wipe).

b) All mobile devices and SIMs provided by V2Soft remain the property of V2Soft at all times.
c) The assigned user will be responsible for the security of the device, SIM card and any accessories. The device must not be passed to another employee for use without prior consultation with the Head of Department and infrastructure team. (Except in an emergency.)
d) Mobile users should protect the device from unauthorised access by setting the password.
e) Data Tethering - Mobile phones cannot be utilised to enable 3G/4G data connection to a Laptop/mobile devices instead of a V2Soft Data Dongle.

The above criteria also apply to SIMs provided for use in Employee own devices. The asset register of mobile devices will be kept by Infrastructure team

5 Responsibility and Ownership

It is the responsibility of approvers, finance/accounts administrators and the user to ensure the guidelines are adhered to.

- It is the responsibility of the user to ensure the security, proper usage and maintenance of any device issued. The mobile device must only be used for business purposes except for use in emergencies and incidental personal use.
- The Infrastructure team will support for internet access, retrieval of email and calendar if appropriate for your device, and other apps approved by V2Soft.
- It is the responsibility of the finance/accounts to monitor usage of mobile devices and ensure that the guidelines are being adhered to.
- The mobile device and data dongle will be logged and registered against the employee.
- The mobile device and data dongle will remain the property of the V2Soft. Under no circumstances will the ownership of the mobile device be transferred to an Employee.
- The Employees are expected to use the device in a responsible manner. Costs due to the loss or damage to the mobile device or Data dongle will be paid by the employee. It will be at the Head of Department’s sole discretion to waive these costs.
- The mobile device and SIM card should not be separated at any time as they are recorded by the service provider and if separated may be disconnected or the warranty invalidated. Users should not swap SIM cards or any equipment without the prior written permission from management. In addition, users should not remove SIM cards from USB Dongles with the intention of making calls via a mobile phone.

- Under no circumstances should a mobile device be dismantled or tampered with in such a way that would lead to the warranty being deemed null and void.

The mobile device and data dongle must be returned to infrastructure by the employees when an employee leaves V2Soft or there is a change in the job role which does not require the use of a mobile device. The device will be put in to a pool of spare devices for re-allocation.

5.1 Mobile Phone and Internet Dongle Use Abroad OR in different region

All Company Mobile Phones and Internet Dongles are barred from being used abroad unless the network provider has been specifically instructed by the Company. In the event that a bar needs to be lifted, please contact your supervisor / HR in order that this may be considered.

It is particularly important on Smartphones to ensure that "data roaming" is switched off for any times. "Data roaming" charges from abroad/different region can result in very high level charges, and if it is found that these have been incurred due to personal use or negligence on the part of the user, then the charges may be passed on to the user.

5.2 Lost or Stolen Mobiles and Internet Dongles

The user is responsible always for the security of the mobile phone and Internet Dongle. It should never be left unattended.

If the phone or Internet Dongle is lost or stolen, this must be reported to HR and IT immediately (if during working hours) by official email, or if out of office hours call service provider directly and ensure that the account is stopped and there is no unauthorised usage.

In the event of loss/theft of a mobile phone or Internet Dongle, the incident must also be reported to the police in co-ordination with V2Soft HR and a FIR should be obtained.

The Company reserves the right to claim reimbursement for the cost of the phone or Internet Dongle, or excess usage charges should the correct procedures not be followed, a user reports repeated loss of their mobile / Internet Dongle, it is deemed that the user has not taken appropriate measures to safeguard the device, or reported the loss thereof (which will be investigated by the Company and judged at its absolute discretion).

5.3 Support

Should there be any queries on the use of the company mobile / Internet Dongle, please contact IT.

5.4 Personal Mobiles and Internet Dongles

Due to the nature of the work environment, personal Mobile Phones, Internet Dongles and hotspots must not be used on Company premises under any circumstances unless authorised in writing by the Director or respective supervisor. Where employee bring a mobile phone onto the premises, it must be kept in silent mode or inactive prior to entering the office premises to avoid any potential problem with Company equipment. Should a personal mobile phone/ Internet Dongle be damaged or stolen while on the premises the Company will not be held responsible for this.

In the event of an emergency, employee should use a Company telephone. If there is a need to be contacted while on duty, this should be via the company’s main telephone number.

Unauthorised use of a personal mobile phone/ personal Internet Dongle during working hours may result in a disciplinary warning or dismissal, depending on the circumstances.

5.5 Industry Best Practices- Pre-requisites:

1) Before configuring the mobile devices for remote access, users should back up all data and verify the validity of the backups. Every telework device’s existing configuration and environment is unique, so changing its configuration could have unforeseen consequences, including loss of data and loss of device or application functionality.
2) Before teleworking, users should understand not only their organization’s policies and requirements, but also appropriate ways of protecting the organization’s information that they may access.

3) Teleworkers should ensure that all the devices on their wired and wireless home networks are properly secured, as well as the home networks themselves.
4) Teleworkers who use their own desktop or laptop PCs for telework should secure their operating systems and primary applications.
5) Teleworkers who use their own consumer devices for telework should secure them based on the security recommendations from the devices' manufacturers.
6) Teleworkers should consider the security state of a third-party device before using it for telework.

5.6 Remote VPN Access

Virtual private network (VPN):

A VPN is a secure "tunnel" that connects the teleworker's computer to the organization's network. Once the tunnel has been established, the teleworker can access many of the organization's computing resources through the tunnel. The types of VPNs most commonly used for teleworking are as follows:

Secure Sockets Layer (SSL) VPN:

Some SSL VPNs primarily provide access to Web-based applications through standard Web browsers. Other SSL VPNs are very similar to IPsec VPNs and can provide access to many types of applications; these types of VPNs typically require users to install additional software.

5.7 Mobile Device Security Overview:

In today's computing environment, there are many threats to telework devices. These threats are posed by people with many different motivations, including causing mischief and disruption, and committing identity theft and other forms of fraud. Teleworkers can increase their devices' security to provide better protection against these threats.

- The primary threat against most telework devices is malware. *Malware*, also known as *malicious code*, refers to a computer program that is covertly placed onto a computing device with the intent of compromising the confidentiality, integrity, or availability of the device's data, applications, or OS. Common types of malware threats include viruses, worms, malicious mobile code, Trojan horses, rootkits, and spyware. Malware threats can infect devices through many means, including email, Web sites, file downloads and file sharing, peer-to-peer software, and instant messaging.
- Another common threat against telework devices is the loss or theft of the device. Someone with physical access to a device has many options for attempting to view the information stored on it.

Security protections, also known as *security controls*, are measures against threats that are intended to compensate for the device's security weaknesses, also known as *vulnerabilities*. Threats attempt to take advantage of these vulnerabilities.

Phones and other mobile devices often contain information, such as email addresses, phone numbers, or your password. Treat your mobile phone just like you would your wallet/ purse or credit card. Keep them either with you or lock them when not in use. Even with the utmost care and attention it is very easy to lose a mobile phone. Mobile devices are valuable, not just in themselves, but because of the data they can hold. Security is required to adequately protect data processed and transferred using mobile devices.

5.8 Mobile device Physical Protection

Using physical security controls for telework devices and removable media. V2Soft Pvt Ltd. require that laptops be physically secured using cable locks when used in hotels, conferences, and other locations where third parties could easily gain physical access to the devices.

V2Soft Pvt Ltd have physical security requirements for papers and other non-computer media that contain sensitive information and are taken outside the organization's facilities.

5.9 Restriction of software installation

A PC/ Laptop can be configured with user accounts and passwords to restrict who can use the PC/Laptop.

The IT team is authorized to install the approved, licensed software. The teleworker is discouraged from installing any software on the PC/Laptop.

5.10 Requirements for mobile device software versions and for applying patches

Many threats take advantages of vulnerabilities in software on PCs. Software manufacturers release updates for their software to eliminate these vulnerabilities. Accordingly, teleworkers should ensure that updates are applied regularly to the major software on their telework PCs.

In addition to the OS, updates should include the following types of software:

- Web browsers
- Email clients
- Instant messaging clients
- Antivirus software
- Personal firewalls

5.11 Restriction

On most OSs, user accounts can have full privileges or limited privileges. Accounts with full privileges, also known as *administrative accounts*, should be used only when performing PC management tasks, such as installing updates and application software, managing user accounts, and modifying OS and application settings. If a PC is attacked while an administrative account is in use, the attack will be able to inflict more damage to the PC. Therefore, user accounts should be set up to have limited privileges; Teleworkers should not use administrative accounts for general tasks, such as reading email and surfing the Web, because such tasks are common ways of infecting PCs with malware.

5.12 Cryptographic controls

Encrypting files stored on telework devices and removable media such as CDs and flash drives. This prevents attackers from readily gaining access to information in the files. Many options exist for protecting files, including encrypting individual files or folders, volumes, and hard drives. Generally, using an encryption method to protect files also requires the use of an authentication mechanism (e.g., password) to decrypt the files when needed.

5.13 Malware protection

The most effective tool for protecting PCs against malware is antivirus software, which is specifically designed to detect many forms of malware and prevent them from infecting PCs, as well as cleaning PCs that have already been infected. Because malware is the most common threat against PCs, The antivirus software should be kept up-to-date.

Configuring antivirus software to use the following types of functions:

- Automatically checking for and acquiring updates of signature or data definition files at least daily
- Scanning critical OS components, such as start-up files, system basic input/output system (BIOS), and boot records
- Monitoring the behaviour of common applications, such as email clients, Web browsers, file transfer and file sharing programs, and instant messaging software
- Performing real-time scans of each file as it is downloaded, opened, or executed
- Scanning all hard drives regularly to identify any file system infections, and optionally scanning removable media as well
- Handling files that are infected by attempting to *disinfect* them, which refers to removing malware from within a file, and *quarantining* them, which means that files containing malware are stored in isolation for future disinfection or examination
- Logging all significant events, such as the results of scans, the start-up and shutdown of antivirus software, the installation of updates, and the discovery and handling of any instances of malware.

5.14 Remote disabling, erasure or lockout

If a cell phone or PDA is lost or stolen, occasionally its contents can be erased remotely. This prevents an attacker from obtaining any information from the device. The availability of this service being depends on the capabilities of the product and the company providing network services for the product the control is not yet implemented.

5.15 Backups

Ensure that information stored on telework devices is backed up. If something adverse happens to a device, such as a hardware, software, or power failure or a natural disaster, the information on the device will be lost unless it has been backed up to another device or removable media.

V2Soft Pvt Ltd. permit teleworkers to back up their local files to a centralized system (e.g., through VPN remote access) and does not recommend the teleworkers perform local backups (e.g., burning CDs, copying files onto removable media).

Teleworkers should perform backups, following the organizations' guidelines, and verify that the backups are valid and complete.

It is important that backups on removable media be secured at least as well as the device that they backed up. For example, if a computer is stored in a locked room, then the media also should be in a secured location; if a computer stores its data encrypted, then the backups of that data should also be encrypted.

5.16 Abuse

Any Employee found to be abusing the usage or care of a mobile device may have the device removed for a defined or indefinite period. Any fines incurred, for example fines by traffic enforcement for the use of mobile devices in certain restricted areas and while driving, will be charged to the users. Such fines cannot be paid from V2Soft funds or reimbursed through an expense claim.

5.17 Problems and Faults

Employee who have a problem with their mobile device or the service can contact Infrastructure Support via the IT service desk for service and advice.

6 Disposal, legacy, resignations and termination

It is the responsibility of the Manager/HR to ensure that any device and SIM are returned to Infrastructure support team when an employee leaves. It should be noted that user contracts are transferable and therefore consideration should be given to whether it is actually necessary to terminate the contract. Transferability provides for the opportunity to re-register the existing mobile or data dongle device and contract to a new user who need not be in the same facility or Service unit.

Devices that have reached the end of life must be disposed of legally as they fall under the regulations and can be considered commercial waste. All end of life devices must be returned to Infrastructure service for disposal and data wiping/reset to factory settings.

7 Health and Safety

7.1 Using Mobile Devices whilst driving

The user must ensure they have full control of any vehicle that they are driving at all times.

It is an offence to use hand held Mobile Phones while driving or while the engine is turned on. The user will be liable for prosecution if they are holding a mobile phone, or any other type of hand held device to send or receive any sort of data, be it voice, text or pictorial images. The user will be regarded to be driving if they are in charge of a vehicle with its engine running on a public road, even if the vehicle is stationary. It is therefore strictly forbidden for the user to use a hand held mobile phone while driving.

A mobile phone may only be used where there is an in-coming call or an out-going voice activated call through a hands-free device that is activated without a need to hold the phone at any time, in which case the call should be kept to the shortest possible time and only to effect essential communications. When the phone needs to be operated to make, or deal with a call through the hands-free device for longer than receiving or giving a short communication, before doing so the user must stop and park the vehicle where it is safe and lawful to do so and with the engine switched off. While driving, they must not use the text message facility on the mobile phone, or if available through such a phone, an image facility or internet access.

Individuals are personally responsible for the payment of any fine or fixed penalty (including any externally raised admin charges) incurred while in charge of the vehicle.

It should be noted carefully that a breach of the Company’s rules on the use of a mobile phone while driving may render the user liable to action under the Disciplinary Procedure.

8 Reference

The following policy documents are directly relevant to this policy, and are referenced within this document:

- V2Soft Remote Work Policy
- V2Soft ISMS Policy
- V2Soft Acceptable Usage Policy
- V2soft Data Protection Policy

9 Policy Violation

Any Violation of this Policy will attract disciplinary action as per V2Soft Pvt. Policies.

10 Policy review

This policy is owned by V2Soft Pvt Ltd. its effectiveness will be monitored and may be reviewed by the company annually. Updates will be notified to all company mobile phone and company Internet Dongle users.