Cell Phone Use Policy

1. **POLICY**

Use of cell phones and other personal electronic mobile devices during work time is a distraction that can create health and safety hazards, disrupt business operations, reduce productivity and compromise personal privacy, customer private data and ABC Company confidential and proprietary information. Accordingly, employees may not use such devices in the workplace or while performing work operations except as provided for under this Policy.

2. **PURPOSE**

The purpose of this Policy is to establish clear ground rules for personal cell phone use at work in the interest of maximizing workplace health and safety, efficient business operation, employee productivity, privacy and confidentiality.

3. **DEFINITION OF CELL PHONE**

For purposes of this Policy, “cell phone” means any handled electronic device capable of receiving and/or transmitting voice, text, or data messages without a cable connection, including, but not limited to, cellular phones, The Company reserves the right to modify or update these policies at any time.

- Cellular and smart phones;
- Digital wireless phones;
- Radio-phones/walkie-talkies;
- Telephone pagers;
- Personal digital assistants with wireless communications capabilities (PDAs); and
- Research in Motion (RIM) wireless devices.

4. **WHOM THIS POLICY COVERS**

This Policy applies to all ABC Company employees, including full-timers, part-timers, temporary employees, independent contractors, dependent contractors, consultants,

interns and volunteers, as well as to workers of vendors and contractors engaged to perform work operations at ABC Company worksites.

5. **PERMITTED CELL PHONE USES**

Employees are expected to focus on work when they are on duty, whether at ABC Company work facilities, while driving or at an offsite location. Use of cell phones is permitted during lunch, coffee and other breaks, provided that it does not disrupt or distract other workers. Employees should instruct and ensure that their friends are aware of and respect these restrictions on personal calls. While on duty, employees are expected to exercise the same discretion in using personal cell phones as they use with ABC Company phones. Employees should not bring their personal cell phones to business meetings, unless they set the device for vibration mode. Employees should also be aware that if they bring personal cell phones to work, they do so at their own risk and that ABC Company is not liable for the loss, theft or damage to personal cell phones brought into the workplace.

6. **PROHIBITED CELL PHONE USES**

- 01 **General**

While on duty, employees may not use their cell phones to make or receive personal calls, emails or texts (except in an emergency), play games, shop for personal purposes, surf the internet or engage in other non-work-related and distracting activities.

- **Cell Phone Use While Driving**

For purposes of safety, employees may not make or receive (or check for) calls, texts, emails or other communications using a cell phone or similar device while driving, regardless of whether the device is hands on or hands off, and whether the communication is personal or job-related. Employees must be aware of when co-workers are driving and refrain from calling, texting, emailing or otherwise reaching out to them during such times. While operating a vehicle, employees may not answer a ring, beep or other cell phone notification signal unless and until they pull over in a safe spot (or let a passenger answer the call). If urgent, employees may accept or return the call, provided that they remain parked off the roadway. They may not resume driving until their conversation is over. Employees may not make outgoing calls while driving and must first pull over in a safe spot before placing the call.

- **Other Dangerously Distracting Uses**

Employees may not a cell phone or similar device while at any work site at which the operation of such device would be a distraction to the user and/or could create an unsafe work environment, such as while operating machinery, handling hazardous products or serving as a traffic controller, confined space attendant or other function requiring 100% focus.

- **Unauthorized Photographs, Videos or Recordings**

Employees may not use any cameras, video and audio recording devices, or video or recording features of cell phones, MP3 Players or Personal digital assistants with wireless communications capabilities (PDAs) or other digital devices that contain such capability at work that can cause violations of privacy and breaches of

confidentiality. Camera phones can present risks to a company, potentially compromising customer information. Use of a cell phone camera to photograph a co-worker, customer, client, visitor, business operation, ABC Company documents, customer or client data or any aspect of ABC Company business without the subject's consent and Company authorization will be subject to disciplinary action, up to and including termination of employment. The same restrictions apply to video and audio recordings.

- **Unauthorized Access**

Access to ABC Company corporate IT networks is a privilege, not a right. Employees seeking to connect their personal cell phone or similar device to the Company network must secure appropriate authorization in accordance with and comply with all rules, regulations and requirements set forth in the ABC Company Mobile Device Acceptable Use Policy.

7. **DISCIPLINE FOR NONCOMPLIANCE**

Failure to comply with any aspect of this Policy will be grounds for discipline in accordance with the protocols and procedures set forth in the ABC Company Progressive Disciplinary Policy.

1. **Violations:** Workers who violate this policy will be subject to disciplinary measures up to and including dismissal, depending on the circumstances.

I have read and will abide by the terms of this policy regarding the use of communication devices at work.

Name (printed) _____

Signature _____ Witness _____

Date _____ Date _____

8. **MOBILE DEVICE USERS' RESPONSIBILITIES**

All mobile device users must:

- Immediately report any lost or stolen devices or unauthorized access to a mobile device or ABC Company data;
- Not use mobile devices that are "rooted" or have unauthorized software/firmware installed;
- Not load illegal content or pirated software onto any mobile device;
- Use only approved applications on mobile devices that connect to the ABC Company network;
- Keep their mobile devices and applications up-to-date;
- Install operating system and application patches within 30 days of release;
- Ensure their mobile devices have active and up-to-date anti-malware/virus protection software;
- Ensure their mobile device physical storage partitions are encrypted;
- Ensure personal firewalls are installed and active, if available;
- Use only ABC Company corporate email systems when sending or receiving ABC Company data;
- Ensure all important files stored on the mobile device are backed up on a

regular basis; and
- Not modify configurations without express written authorization from [*insert appropriate person or position*]; and
- Attend a training session about this Policy.

9. **ACCESS CONTROL**

- 01 **Connection Rights**

The ABC Company IT department reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure and will engage in such action if such equipment is being used so as to put the Company's systems, data, users and clients at risk.

- **Approval of Mobile Devices**

All mobile devices must be approved by IT before initial use on the corporate network or related infrastructure. ABC Company will maintain a list of approved mobile devices and related software applications and utilities, which IT may update from time to time. The list will be stored at [*file location or URL*]. Devices that are not on this list may not be connected to corporate infrastructure. If your preferred device does not appear on this list, contact [*list contact and contact information*].

- **End Users' Responsibilities**

End users wishing to connect such devices to non-corporate network infrastructure to gain access to enterprise data must follow whatever security measures deemed necessary by the IT department with regard to their devices and related infrastructure. Enterprise data may not be accessed on any hardware that does not meet ABC Company's established enterprise IT security standards.

- **Internet Access**

Personal mobile devices may not be connected to the corporate network through the Internet unless and until they are inspected by IT. Devices not approved by IT will not be allowed to connect. Devices may only access the corporate network and data through the Internet using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal web address will be provided to users as required. Smart mobile devices such as smartphones, tablets, and laptops must access the corporate network and data using mobile VPN software installed on the device by IT.

- **Prohibited Devices & Applications**

The following devices and applications may not be used in the workplace or in conjunction with ABC Company data:

- Location-based services and mobile check-in services which use GPS capabilities to share real-time user location with external parties;
- Mobile devices to capture images, video, or audio, whether native to the device or through third-party applications; and
- Applications that are not approved by IT.

10. **MEDICAL DEVICE MANAGEMENT**

The IT department uses the [*insert*] mobile device management (MDM) solution to secure

mobile devices and enforce policies remotely. Before connecting a mobile device to ABC Company resources, the device must be set to be manageable by [*insert*]. [*Insert*]'s client application must be installed on any mobile devices connecting to ABC Company resources, including personal devices owned by employees. The MDM solution enables IT to take the following actions on mobile devices: [*remote wipe, location tracking, remote lock*]. Any attempt to contravene or bypass the MDM implementation will result in immediate disconnection from all ABC Company resources, and may result in discipline in accordance with ABC Company IT Security and Progressive Discipline policies.

11. **SECURITY**

All employees using mobile devices and related software for network and data access must use secure data management procedures. IT will manage security policies, network, application and data access centrally using whatever technology solutions it deems suitable.

- **Passwords & Encryption**

All mobile devices must be protected by a strong password, and not simply a PIN. All data stored on the device must be encrypted using strong encryption following ABC Company's Password & Encryption Policy. Employees agree never to disclose their passwords to anyone. Passwords and other confidential data, as defined by IT, may not to be stored unencrypted on mobile devices.

- **Physical Security**

All users of mobile devices must use reasonable physical security measures. End users must secure all such devices from being lost or stolen, both when they are actually in use and when they are being carried. Employees, contractors, and temporary staff must follow all enterprise-sanctioned data removal procedures to permanently erase Company-specific data from their devices once its use is no longer required.

- **Lost or Stolen Devices**

User must immediately report any lost or stolen mobile device to IT immediately. Such lost or stolen devices will be remotely wiped of all data and locked to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning. The remote wipe will destroy all data on the device, whether it is related to company business or personal.

- **Remote Wipe Waiver**

Before connecting before connecting the device to ABC Company corporate resources, users must agree to and sign the ABC Company Remote Wipe Waiver acknowledging their understanding and agreement that personal data may be erased in the event of a security breach.

- **Anti-Virus Software**

All non-corporate computers used to synchronize or backup data on mobile devices must have installed up-to-date anti-virus and anti-malware software deemed necessary by IT.

- **Authentication**

Any mobile device used to store or access ABC Company data must meet the authentication requirements of IT. All hardware security configurations must be pre-approved by IT before any enterprise data-carrying device can be connected to the corporate network.

- **Internet Access**

Employees, contractors and temporary staff accessing ABC Company internet resources from a smartphone or tablet may NOT save their user credentials or internet sessions when logging in or accessing Company resources of any kind.

12. **HARDWARE & SUPPORT**

IT will support the connection of mobile devices to ABC Company corporate resources, but IT will not support hardware issues or non-corporate applications on personally owned devices. In addition, IT has the right and responsibility to use any means it considers necessary to limit the ability of end users to transfer data to and from specific resources on the enterprise network. Users may make no modifications to the hardware or software that change the nature of the device in a significant way (e.g., replacing or overriding the operating system, jail-breaking, rooting) without IT's express approval.

13. **AUDIT TRAILS**

IT will establish audit trails, which will be accessed, published and used without notice, to track the attachment of an external device to the corporate network, and the resulting reports may be used for investigation of possible breaches or misuse. End users agree to and accept that their access and/or connection to ABC Company networks may be monitored to record dates, times, duration of access, etc., for purposes of identifying unusual usage patterns or other suspicious activity. The status of the device, including location, IP address, Serial Number, IMEI, may also be monitored. This monitoring is necessary to identify accounts/computers that may have been compromised by external parties or users who are not complying with ABC Company policies. End users understand and acknowledge that **they have no reasonable expectations of privacy** in that or any of the forgoing or other information related to their access, connection to and use of the device and accompanying media.

14. **DISCIPLINE FOR NONCOMPLIANCE**

Failure to comply with any aspect of this Policy will be grounds for discipline up to and including termination in accordance with the protocols and procedures set forth in the ABC Company Progressive Disciplinary Policy.

15. **EMPLOYEE ACKNOWLEDGEMENT**

I, [*employee name*], have read and understand the above Cell Phone Use Policy, and agree to comply with the rules and provisions it contains.

_____
_____

Employee
Signature
Date