Mobile Device Access & Use Policy

Janco Associates, Inc.

2024

Table of Contents

Mobile Access and Use Policy

Overview

Business mobile usage is exploding and becoming an increasingly powerful tool for marketers to connect with consumers around the world. Statistics show that professional text message use is expected to continue growing through the end of this decade. Although few in-depth studies focused on text messaging statistics have been done in the past, recent reports are beginning to shed light on the opportunities and help us grasp the size and potential impact on businesses.

- 5 billion people globally send and receive SMS messages.
- Over 300 million people in North America use text messages
- The mobile industry had a revenue of $2 trillion last year
- 3.3 billion people access the internet via mobile. It's predicted that by 2030, 72.6% of internet users will access the web via mobile-only, using their smartphones.
- 4 billion people are expected to own a smartphone by the end of the decade

's technology-based resources (such as
c.) from unauthorized use and/or malicious
itical applications, loss of revenue, and
wireless methods of accessing corporate
cesses for doing so.

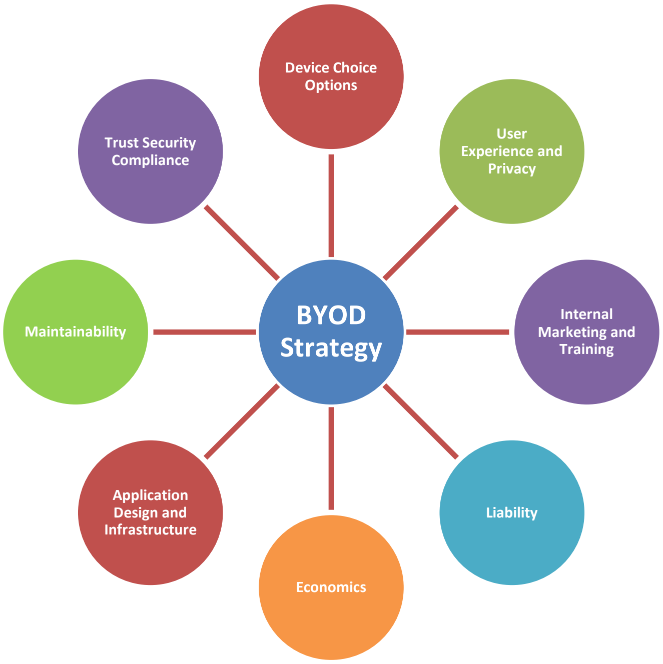
s, and restrictions for end-users who have
terprise data from a mobile device connected via a wireless or unmanaged network outside of ENTERPRISE's direct control. This policy applies to, but is not limited to, all devices and media that fit the following device classifications:

- Smartphones
- PDAs
- USB applications and data
- Laptop/notebook/tablet computers
- Ultra-mobile PCs (UMPC)
- Mobile/cellular phones
- Home or personal computers used to access enterprise resources
- BYOD
- Wearable Devices
- Any mobile device capable of storing corporate data and connecting to an unmanaged network

The policy applies to any hardware and related software that could be used to access enterprise resources, even if the equipment is not approved, owned, or supplied by ENTERPRISE.

With the advent of BYOD (Bring Your Own Device) and Wearable Devices, the implications for privacy, security, compliance, and record management are significantly more complex. However, this full policy does apply to those devices as well.

Components of the BYOD Strategy and Basics for BYOD Policy


Device Choice Options
User Experience and Privacy
Internal Marketing and Training
Liability
Economics
Application Design and Infrastructure
Maintainability
Trust Security Compliance
BYOD Strategy

A BYOD strategy and r xperience and privacy; internal marketing and maintainability; and trust security complia policy. A detailed description of each of

Device

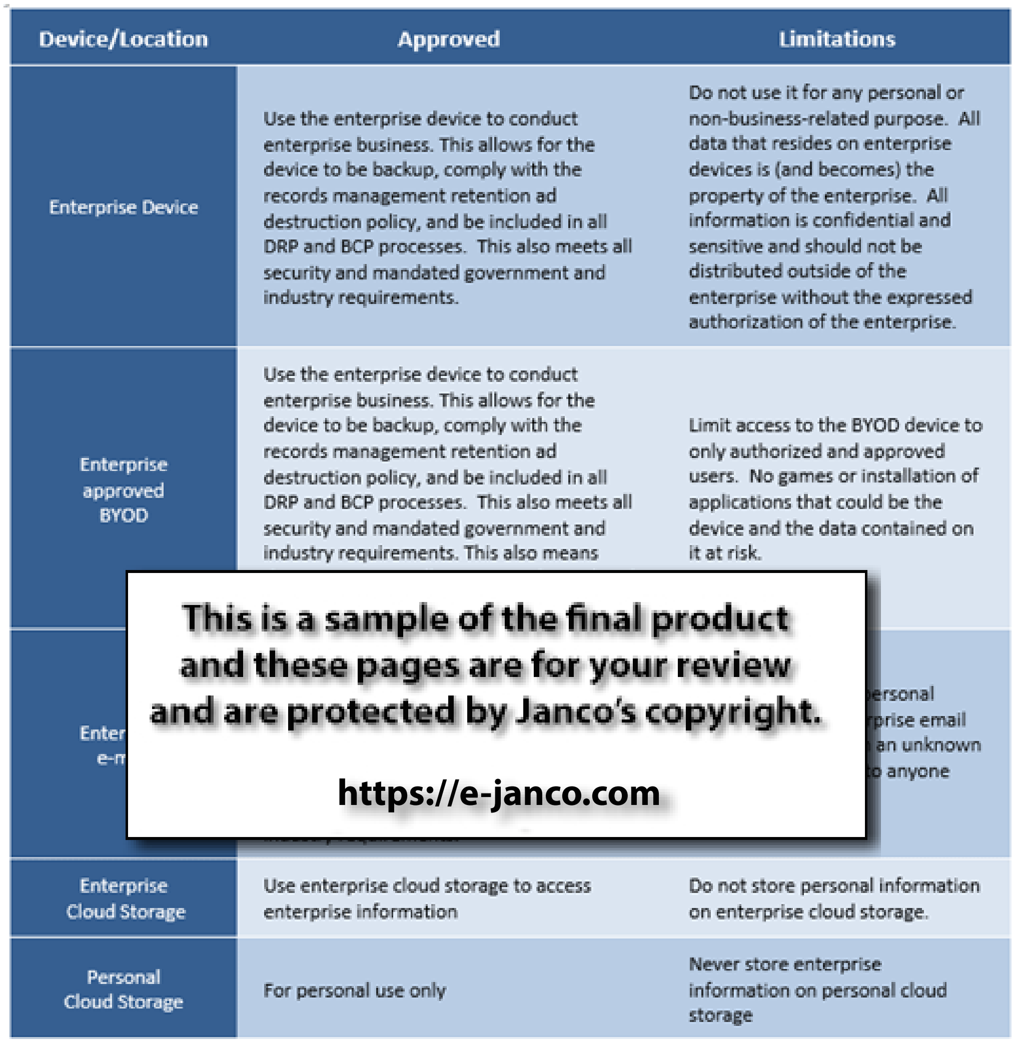
- Analyze employee preferences and understand which devices they already have
- Definite an acceptance baseline of what security and supportability features a bring-your-own-device program should support
- Understand the operating system, hardware, and regional variances around that baseline
- Develop an “easy” certification process for the evaluation of future devices
- Establish clear communication to users about which devices are allowed or not, and why

Mobile Devices

Regardless of whether individuals work on their tablets, PDAs, or SmartPhones (see list above) or are corporate-issued ones, the policy of ENTERPRISE is that these users must follow IT to support the management, tracking, securing, and supporting of these devices, just like they do for any other corporate computing platform.

Specifically, the policies that apply to these types of devices are:

- Comply with security best practices for tablets, including the use of multilevel passwords and device certificates, and the ability to remotely wipe the device if it is lost or stolen.
- Utilize tiered access to network resources to secure critical data and applications.
- Comply with application delivery mechanisms.



Device/Location	Approved	Limitations
Enterprise Device	Use the enterprise device to conduct enterprise business. This allows for the device to be backup, comply with the records management retention ad destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements.	Do not use it for any personal or non-business-related purpose. All data that resides on enterprise devices is (and becomes) the property of the enterprise. All information is confidential and sensitive and should not be distributed outside of the enterprise without the expressed authorization of the enterprise.
Enterprise approved BYOD	Use the enterprise device to conduct enterprise business. This allows for the device to be backup, comply with the records management retention ad destruction policy, and be included in all DRP and BCP processes. This also meets all security and mandated government and industry requirements. This also means	Limit access to the BYOD device to only authorized and approved users. No games or installation of applications that could be the device and the data contained on it at risk.
Enter e-m	[illegible]	ersonal rprise email an unknown o anyone
Enterprise Cloud Storage	Use enterprise cloud storage to access enterprise information	Do not store personal information on enterprise cloud storage.
Personal Cloud Storage	For personal use only	Never store enterprise information on personal cloud storage

Electronic Forms

Nine (9) electronic forms are included with this policy template. They come separately in their directory.

- BYOD Access and Use Agreement Form
- Company Asset Employee Contol Log
- Employee Termination Checklist
- Mobile Device Security Access and Use Agreement Form
- Mobile Device Security and Compliance Checklist
- Wearable Device Access and Use Agreement
- Work From Home Contact Information
- Work From Home IT Checklist
- Work From Home Work Agreement

What's New

2024 Edition

- Updated all attached forms
- Updated Employee Termination Checklist

2023 Edition

- Updated all attached forms
- Updated Employee Termination Checklist
- Updated to reflect changes due to the remote workforce
- Defined mobile device, BYOD, and Cloud uses and limitations

2022 Edition

- Updated all attached forms
- Added Employee Termination Checklist
- Updated to reflect changes due to the remote workforce
- Define ownership rules

2021 Edition

- Updated all attached forms
- Updated to reflect WFH
- Added four (4) forms
    - Wearable Device Access and Use Agreement
    - Work From Home Contact Information
    - Work From Home IT Checklist
    - Work From Home Work Agreement

2020 Edition

- Updated all the forms to the latest version which meets all mandated security and privacy requirements
- Updated to meet CCPA mandates