Sample Corporate Mobile Device Acceptable Use and Security Policy

Get an inside look at what other companies are doing with this actual BYOD policy from a Fortune 1000 Insurance Company

WISEGATE MEMBER CONTRIBUTED CONTENT

A 451 Research® Community
Introduction

Securing corporate information while allowing employees to use their personal mobile devices on the corporate network is still a major challenge for most companies. Knowing how to create mobile device policies that balance the needs of both employees and the company is difficult.

Originally developed by a Wisegate member from a Fortune 1000 Insurance company, this sample Corporate Mobile Device Acceptable Use and Security Policy can help you get started in creating or updating your own policy.

With exclusive access to a vetted group of senior-level IT security professionals, Wisegate members are able to gain insights into what their peers are doing and learn from their successes and failures. This sample Corporate Mobile Device Acceptable Use and Security Policy is an example of the kind of information Wisegate members typically share with each other.

Would you like to join us? Go to wisegateit.com to learn more and to submit your request for membership.
# Table of Contents

**Policy Development Project Introduction** ................................................................. 4  
  - Material Under Review or Development ................................................................. 4  
  - Active Policy ............................................................................................................. 4  
  - Objective and Scope ................................................................................................ 4  

**End-User Policy** ........................................................................................................ 5  
  - Policy Artifact ......................................................................................................... 5  
  - Technical Policy ...................................................................................................... 9  

**Secure Configuration Policy** ..................................................................................... 10  
  - Blackberry Device Support .................................................................................... 10  
  - Apple Device Support ............................................................................................ 10  
  - Android Device Support ....................................................................................... 10  
  - Mobile Device Application Development ............................................................ 10  
  - General Information Security Controls ................................................................. 10  

**Socialization and Communication Plan** .................................................................. 18  
  - Review Ladder ........................................................................................................ 18  
  - Authorization .......................................................................................................... 21  
  - Communications and Publishing Plan .................................................................... 21
Policy Development Project Introduction
The purpose of this document is to facilitate the development and review of Corporate Information Security Policies, Standards, Procedures and other control matter relevant to Corporate information security posture.

Material Under Review or Development
A description of the control material (policy, standard, process, guideline, directive, etc.) under review.

Mobile Device Acceptable Use & Security Policy

Active Policy
The written material actively affecting control. This is typically a policy, standard, process, guideline, directive, etc.

User Policy
Smartphone Acceptable Use Policy version XX. (link to published material)

Configuration Policy
Wireless Device Communications and Connectivity version XX. (link to published material)

Objective and Scope
The objective is to endorse and enable for Corporate business use:

• Personally owned mobile devices
• Corporate owned mobile devices

Policy Development Team

<table>
<thead>
<tr>
<th>Member</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Project Facilitation; Research; Policy Release</td>
</tr>
<tr>
<td></td>
<td>Candidate Preparation</td>
</tr>
<tr>
<td></td>
<td>Advisor: Information Security SME; CISO</td>
</tr>
<tr>
<td></td>
<td>Technical Operations</td>
</tr>
<tr>
<td></td>
<td>ITS</td>
</tr>
<tr>
<td></td>
<td>ITS</td>
</tr>
<tr>
<td></td>
<td>CIO; Policy Approval</td>
</tr>
</tbody>
</table>
End-User Policy

Policy Artifact
This section contains the policy content that will be published to all employees.

Policy Title

<table>
<thead>
<tr>
<th>Existing</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartPhone Acceptable Use Policy</td>
<td>Mobile Device Acceptable Use and Security Policy</td>
</tr>
</tbody>
</table>

Purpose

The purpose of this policy is to establish the criteria governing the authorized use of personal or corporate owned smartphone and tablet (mobile) devices where the owner has established access to the Company’s Systems enabling them to send and receive work-related e-mail messages and conduct other company business.

Policy Statement

Employees may use approved personally owned and corporate owned mobile devices to access the Company messaging system and the approved Corporate wireless network as necessary in the course of their normal business routines in support of the Company's published goals and objectives.

User Responsibility

General

User agrees to a general code of conduct that recognizes the need to protect confidential data that is stored on, or accessed using, a mobile device. This code of conduct includes but is not limited to:

- Doing what is necessary to ensure the adequate physical security of the device
- Maintaining the software configuration of the device – both the operating system and the applications installed.
- Preventing the storage of sensitive company data in unapproved applications on the device.
- Ensuring the device’s security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes
- Reporting a lost or stolen device immediately
Personally Owned Devices

The personal smartphone and tablet devices are not centrally managed by Corporate IT Services. For this reason, a support need or issue related to a personally owned device is the responsibility of the device owner. Specifically, the user is responsible for:

- Settling any service or billing disputes with the carrier
- Purchasing any required software not provided by the manufacturer or wireless carrier
- Device registration with the vendor and/or service provider
- Maintaining any necessary warranty information
- Battery replacement due to failure or loss of ability to hold a charge
- Backing up all data, settings, media, and applications
- Installation of software updates/patches
- Device Registration with Corporate IT Services

Corporate Owned Devices

Corporate owned smartphone and tablet devices are centrally managed by Corporate IT Services. Specifically, the user is responsible for:

- Installation of software updates
- Reporting lost or stolen device immediately

Corporate IT Services Support Responsibility

The following services related to the use of a personal smartphone or tablet are provided by Corporate IT Services:

- Enabling the device to access the web-based interface of the email system. This is a default capability. Personal device registration is not required.
- Enabling the device to access the web-based application system. This is a default capability. Personal device registration is not required.
- Email, Calendar and Contact Sync service configuration. Personal device registration is required.
- Wi-Fi Internet Access configuration. This service is limited to the facility. Personal device registration is required. Personal email will not sync when connected to the Company network.
• Devices not compliant with secure configuration standards will be unsubscribed from Mobile Device services.

**Access Registration Requirement**

To comply with this policy the mobile device user must agree to:

• Register the device via Corporate place. “Work Tools, Self Service Tools, Services Request Forms, Technology Service Center Form, Mobile Device Policy Acceptance.”

• Device reset and data deletion rules below.

• Device must be encrypted or user must purchase software to ensure data on the device is encrypted.

• Installation of Mobile Device Management solution on the device (provided by Corporate IT Services).

• Acceptance of Corporate Mobile Device Acceptable Use and Security Policy (this policy).

**Security Policy Requirements**

The user is responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. Removal of security controls is prohibited.

User is forbidden from copying sensitive data from email, calendar and contact applications to other applications on the device or to an unregistered personally owned device.

Security and configuration requirements:

• Sensitive data will not be sent from the mobile device. Encrypted mail services will be utilized in such cases.

• The device operating system software will be kept current.

• The data on the device will be removed after 10 failed logon attempts.

• The device will be configured to encrypt the content.

• The device will be configured to segregate corporate data from personal data.

• User agrees to random spot checks of device configuration to ensure compliance with all applicable Corporate information security policy.
Wi-Fi Access to Corporate Network

Users who connect to the Company Wi-Fi network with a personally owned device will be allowed access to Corporate systems and resources available via the Internet.

Loss, Theft or Compromise

If the device is lost or stolen, or if it is believed to have been compromised in some way, the incident must be reported immediately by contacting Physical Security, the Technology Service Center or a member of the user’s management team.

Company’s Right to Monitor and Protect

The Company has the right to, at will:

- Monitor Corporate messaging systems and data including data residing on the user’s mobile device
- Modify, including remote wipe or reset to factory default, the registered mobile device configuration remotely

Device Reset and Data Deletion

Device user understands and accepts the Company data on the device will be removed remotely under the following circumstances:

- Device is lost, stolen or believed to be compromised
- Device is found to be non-compliant with this policy
- Device inspection is not granted in accordance with this policy
- Device belongs to a user that no longer has a working relationship with the Company. Note: the “selective” wipe capability is available for iOS based devices only. BlackBerry OS based devices will be reset to the factory default.
- User decides to un-enroll from the Mobile Device Policy and Management solution

Enforcement

Any user found to have violated this policy may be subject to disciplinary action, including but not limited to:

- Account suspension
- Revocation of device access to the Company System
- Data removal from the device
• Employee termination

**Technical Policy**
This section reflects changes needed to existing technical policy material.

**Data Segregation on mobile devices**
Corporate data must be kept separate from personal data

**Approved Technology**
All wireless LAN access provisioned to the Company Network must use corporate-approved vendor products and security configurations. Corporate owned assets, and those explicitly allowed per the Mobile Device Policy, are the only devices that can be approved and authorized for use on the Company Network.

Home-based wireless networks are not supported by the Company. If a home-based wireless network is encrypted using WPA or later Corporate equipment may be configured for access to the network.
Secure Configuration Policy

Blackberry Device Support
Blackberry OS based smartphone and tablet devices are supported at this time.

Apple Device Support
- Apple IOS based smartphone and tablet and iTouch devices are supported at this time.
- Only IOS Version XX, XX devices are supported at this time

Un-tethered Jailbreak Risk
Risk and Compensating Control: To address the risk of an un-intentional jailbreak resulting in data compromise no version of the IOS known to be susceptible to a non-tethered jailbreak exploitation will be allowed to remain subscribed to the Company Mobile Media services.

Android Device Support
- Android based smartphone and tablet devices are supported at this time.
- Only Android Version XX, XX devices are supported at this time

Android Risk Information
The Android’s biggest iPhone differentiator is its openness. The Android operating system is more customizable; its application model more open and its app distribution approach is much less restrictive (including a lower approval bar in the Android Market while also allowing apps to be proliferated outside of the market). That freedom opens the door to potential and actual security problems.

Mobile Device Application Development
This policy does NOT address application development or deployment of custom built applications to a mobile device.

General Information Security Controls

Introduction
The mass-adoptation of both consumer and corporate owned mobile devices has increased employee productivity but has also exposed the Company to new security risks. Current control technologies may be insufficient to protect the enterprise assets that regularly find their way onto devices. Complicating the security picture is the fact that virtually all of today’s mobile devices operate in an
ecosystem, much of it not controlled by the Company. Devices connect and synchronize out-of-the-box with third-party cloud services and computers whose security posture is potentially unknown and outside of the Company’s control.

Control Risks

While the decision to allow employees to use mobile and personal devices, to improve productivity and work efficiency, the Company is doing so ever-aware of the risks outlined below:

Sensitive Data Exposure

Exposing sensitive data. As employees use more and different mobile devices in various settings, they are more likely to lose those devices or have them stolen.

Malware

Introducing malware to the Company network. It is already difficult to maintain network security with standardized devices via controlled access. For this reason the Company has screened the multitude of non-standardized devices end-users might wish to connect to the Company network and selected solutions that enable both flexibility and essential controls.

Co-Mingling Corporate and Personal Data

Greater need to control network access and ensure data privacy. When employees leave an organization, or they lose a mobile device, The Company needs to quickly terminate network access and restrict access to corporate data residing on the device.

Corporate Data Segmentation and Encryption

Corporate data must be protected and segmented at all times from the employee’s personal data stored on the device.

Initial Service Control Features and Policy

Essential Access Controls

The essential basic access controls are supported

- Password Strength
- Inactive Device Lockout
- Encryption
- Remote Data Removal
Web Application Access

- Outlook Web Access
- Corporate Applications Portal available via Citrix

Email

Native Email Sync Enabled

- Users enjoy the native email application experience. Allowing mobile devices to access Corporate email systems through the native application is ideal because the native application is designed for the mobile device form factor. Forcing someone to read email using a web-based interface falls short of the user’s expectation. Some security solutions require using web-based access to email or a second non-native email application. The Company policy enables the use of the native email application giving the user the rich functionality they expect.

- **Risk:** Native mobile email applications allow unintentional and malicious movement of email to and from the Company BPOS account and any personal email accounts.

- **Compensating Control:** The problem of data leakage between email accounts on the device is mitigated by the Mobile Device Management (MDM) system. MDM policy will prevent moving email directly between accounts.

Secure Email Send feature – Not Supported

Secure Email feature not supported on mobile devices

- Initial and Annual communications of acceptable use must be communicated to the service user base

Web Filtering – Limited Support

Web filtering services are available on a mobile device at this time only if the device is accessing the Internet via the Company Wi-Fi network.

WiFi Access to Internal Resources - Limited

- Qualified personal devices are allowed to leverage the Company network to access Internet based services

- Access to the Company's Wi-Fi network has been configured to enable a mobile device (corporate owned or personal) to connect, in a logically segregated and secured way (controlled) way, to the Company corporate network. Only Corporate resources already available via the Internet are accessible.
• Personal e-mail access via SMTP on any Corporate Wi-Fi network is not supported

Mobile Device Management

Mobile Device Management (MDM) solutions are the foundation of a secure mobile device deployment.

• MDM makes configuration control possible.
• Risk: MDM solutions are not necessarily security-centric and do not typically cover all the security fundamentals. The MDM tools reality is that most Mobile Device Management solutions provide a set of capabilities that address only some of the security problems presented by Mobile Devices.
• Compensating Control: The essential MDM use cases such as enforcing a pass code, encryption of stored data and wiping a device if it gets lost—are being fulfilled by the MDM vendor selected by the Company.

Corporate and personal data separation

Corporate data will be kept separate from personal data.

User Awareness of Their Responsibilities

All authorized mobile device users will be reminded every six months of their responsibilities.

About Personal Data Access

General Council wishes to understand what access Corporate has to personal data on a personal device.

• Can Corporate monitor or observe the data?
  NO, we have the ability to monitor encryption, security controls, installed applications, app distribution, MDM profiles, Device Jailbroken, but not data—with exception of Corporate configured (e-mail, calendar, contacts).
• Is this access limited to deletion only?
  YES, all Corporate configured data is removed once un-enrolled from MDM or reset to factory default.(this excludes any data manually moved to other applications on the device by the user).

Compliance and Reporting

Compliance and Security Reporting – The security solution must be able to report what controls policy has been deployed, that a device is not “rooted” or “Jailbroken” and that policy controls applied are in still in place.
• Thinking of a mobile device as if it were a laptop or a personal computer also requires one to know if the SD card is encrypted, or if any anti-malware controls are current and running or if someone is accessing illicit web content. The selected controls to enforce security policies on mobile devices must meet these requirements if the Company is to maintain the current information security posture.

Detection and Prevention of Data Leaks

• Data seeping or leaking from/to personally owned devices remains a realm of control concern. This is true for MDM solutions including the solution selected by the Company. It is possible, even with the selected control software in place, to experience data and malware leakage to and from mobile devices through the native email client. This means email and attachments containing sensitive data (PII, M&A futures, Medical claims dialog, etc.) can move from a Corporate managed system to a non-Corporate system easily and intuitively. This exfiltration/infiltration of data can be unintentional or malicious.

• Native mail applications make it simple to file an email from a Corporate email account to a personal Yahoo or Gmail account and vice versa. There are no native controls in place to prevent this. In fact the email application is designed to enable this to make management of multiple email accounts easier for the mobile device user.

• The problem of data leakage between email accounts on the device is mitigated by the Mobile Device Management (MDM) system. MDM policy will prevent moving email directly between accounts.

Patch Management

Security patching is fundamental in the Desktop and Server Management spaces and are required in order to close vulnerabilities as they are discovered and before they are exploited. Some relief comes from the OS vendors who are supposed to keep your device current. The vendor selected by the Company has a way to patch a device, to resolve vulnerability quickly and ensure these devices remain compliant with company security patch management policy.

Archival of Text Messages - Limited

Corporate requirements dictate archiving of all emails and SMS messages sent from a device used to conduct Corporate business. This capability is simply not in place. The deployment team will address the need for users to be educated about the appropriate use of texting apps. It is assumed that mobile device controls will be enhanced to address this problem when the technical means to do so is viable. Update: This capability is simply not in
place for SMS messages but is in place for all e-mail through our standard archival system.

Malware Control

Inevitable malware threats remain a concern on all computing platforms. Mobile devices are not alone here. The Apple IOS provides a software quality ecosystem and “application sandboxing” to counter this threat to some extent.

- If an application in the Apple “App Store” is discovered to be malware, Apple has the ability to “kill” the application and remove it from the installed base. This is a significant deterrent to a would-be iPhone/iPad malware writer. What is the point of writing malware if the planet’s population of IOS devices can be cleaned of it in the span of 24 hours once discovered?
- The Apple IOS also employs a concept known as “application sandboxing” which makes it impossible for one application to invade the domain of another.

Policy Management - Limited

Capabilities in the Policy Management realm are lack luster for mobile devices in general. It is a plus that Apple IOS limits what can be done between applications (as mentioned in the Malware section above). A comparative few (approximately 20) policy control points exist for ActiveSync (among which few are actually considered useful) on mobile devices. Comparatively, there is a myriad of policy attributes and actions that can be applied to a Laptop device or to a BlackBerry device. It is assumed that mobile device controls will be enhanced to address this problem when the technical means to do so is viable.

Deferred Control Features and Policy

Devices Not Supported

The following device platforms and related variants are not supported at this time:

- Symbian OS
- Nokia Maemo/Meego
- Microsoft Windows Mobile
- Microsoft Windows Phone
- Samsung/Bada
- Sony Ericsson
- Motorola
• O2
• Palm OS
• Audiovox
• Any platform not explicitly named in the “Multiple Device Platforms Allowed” section of this document.

Self Service Device Management
• Enrollment of Personal Devices
• Wipe of Lost or Stolen Devices
• Passcode Reset
• Device Locator (where did I put that?)

Backup and Recovery
• What is the responsibility the user has for backing up data?
• What is the state of Corporate data that resides in a device backup file?
• Can Corporate data in a device backup file be restored without the policy oversight?

Application Restrictions
• Games
• Gambling
• Instant Messaging Clients
• Pornography
• Guns

Forensics and Litigation Support Services

Controls Compliance Testing and Reporting
• Manual
• Automatic

Application Providence – Signed by Vendor

Control Validation Testing

Are the policies translating into effective controls, especially when control requires user action?
• Clarification / Control Testing Process?

International Travel Rules

• What are the users responsibilities when traveling outside the Company?
• What are the high-risk countries?
• Post trip practices? Wipe? Rebuilt? Dispose of?

Application Sandboxing – Android Devices

• Are Android based device applications segmented from each other? No

Baseline Security Posture Monitoring and Control

The Company currently inspects non-Corporate laptops to determine the device's security posture before allowing LAN or Wi-Fi network access. The equal level of scrutiny is difficult to apply when inspecting a smartphone or tablet device. This makes it difficult to rationalize some levels of access that normally would be based on those checks. With mobile platforms:

• It can be hard to determine if the latest patches are up to date,
• If it is free of malware,
• If it is free of otherwise unauthorized programs, and
• If it abides by the Company access policy.
• Manually inspecting mobile devices every time one is allowed network access is cost prohibitive.

Different security policies may apply to mobile computing devices than to traditional devices. This is because the management tools and technology lag behind the laptop devices market.

Can the corporation disable the personal device if it is compromised and contains sensitive information? The answer is yes. The device must of course be reported lost or stolen by the end-user.

• Control complications
• Automated security screen upon connection is not supported yet.
• Pre-screening the device’s security posture and making a calculated risk decision is the only way, at this point, to enable non-Corporate mobile devices access to the Company’s network and to allow Corporate email, calendar and contact data to be stored on the device.
Mobile Device Scanning

What is being done to integrate mobile device scanning into our vulnerability management workflow?

Find My Device service integration

What will be done to leverage lost/stolen device location technology in the incident response process?

Socialization and Communication Plan

This Review Ladder describes who the stakeholders are, who will be involved in the review of the proposed matter, and in which draft cycle. This plan is designed to ensure efficient content development and to ensure the proper awareness is in place before expanding the review and ultimately obtaining signoff.

RACI Role Definitions

**Responsible**: Person(s) responsible for effectiveness of the control after implementation.

**Accountable**: Approval authority for the matter content. Final Signatory.

**Consulted**: Those whose opinions are sought; and with whom there is two-way communication and feedback consideration.

**Informed**: Those who are kept up-to-date on progress, often only on completion of the review; and with whom there is just one-way communication. This list used to ensure the right people are aware of the matter/content once completed and approved. The entire table is used to identify who (individuals or groups) will be educated as part of the Communications and Publishing plan above.

Review Ladder

![Phase is complete](checkmark)

![Phase in progress](arrow)

Start Date: MM/DD/YYYY

<table>
<thead>
<tr>
<th>Phase</th>
<th>Stakeholder</th>
<th>Role</th>
<th>Role</th>
<th>Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Candidate 1</td>
<td></td>
<td></td>
<td></td>
<td>Start: MM/DD/YYYY</td>
</tr>
<tr>
<td></td>
<td>Consulted</td>
<td>Research and Initial</td>
<td>MM/DD/YYYY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Responsible</td>
<td>ITS</td>
<td>MM/DD/YYYY</td>
<td></td>
</tr>
<tr>
<td>Release Candidate 2</td>
<td>Accountable (Delegate)</td>
<td>Start: MM/DD/YYYY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------</td>
<td>------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsible</td>
<td>ITS</td>
<td>MM/DD/YYYY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsible</td>
<td>ITS</td>
<td>MM/DD/YYYY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsible</td>
<td>ITS</td>
<td>MM/DD/YYYY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountable (Delegate)</td>
<td></td>
<td>MM/DD/YYYY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consulted</td>
<td>Communications</td>
<td>MM/DD/YYYY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountable</td>
<td>CIO</td>
<td>MM/DD/YYYY</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Release Candidate 3</th>
<th>Accountable (Delegate)</th>
<th>Start: MM/DD/YYYY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible</td>
<td>ITS</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>Responsible</td>
<td>ITS</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>Responsible</td>
<td>ITS</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>Accountable (Delegate)</td>
<td></td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>Accountable</td>
<td>CIO</td>
<td>MM/DD/YYYY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Release Candidate 4</th>
<th>Accountable (Delegate)</th>
<th>Start: MM/DD/YYYY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible</td>
<td>ITS</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>Responsible</td>
<td>ITS</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>Responsible</td>
<td>ITS</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>Accountable (Delegate)</td>
<td></td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>Accountable</td>
<td>CIO</td>
<td>MM/DD/YYYY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Comm. and Publication</th>
<th>Members of previous cycle are copied</th>
<th>Start: MM/DD/YYYY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Informed</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporate Enterprise Policy Council</td>
<td>Informed</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal: HR</td>
<td>Informed</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal: Privacy</td>
<td>Informed</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Authorization

<table>
<thead>
<tr>
<th>Date</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval</td>
<td>MM/DD/YYYY</td>
<td>Default: the date following the final day of last draft review cycle</td>
</tr>
<tr>
<td>Effective</td>
<td>MM/DD/YYYY</td>
<td>Default: same as approval Date</td>
</tr>
<tr>
<td>Review</td>
<td>MM/DD/YYYY</td>
<td>Default: 3 years from effective date</td>
</tr>
<tr>
<td>Completion</td>
<td>MM/DD/YYYY</td>
<td>Target: 5 days after approval date</td>
</tr>
</tbody>
</table>

Approval Matter

Evidence of approval of the new matter is inserted here.

< PDF versions of email messages containing approval are inserted here >

Communications and Publishing Plan

This section describes how the appropriate stakeholders will be notified of the approved control matter.

<table>
<thead>
<tr>
<th>Date</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Approved final artifact will be provided to the change requester</td>
<td>MM/DD/YYYY</td>
<td>Target: 5 days after approval date</td>
</tr>
<tr>
<td>2. Policy Portal update will be made</td>
<td>MM/DD/YYYY</td>
<td>Target: 5 days after approval date</td>
</tr>
</tbody>
</table>