



Whitepaper

January 2011

A Practical Guide to Deploying BlackBerry Policies

A J.Gold Associates White Paper

“Smart phones have become essential tools for business. To maximize their benefits, companies should determine which features and functions are appropriate in the user’s work environment, which capabilities if enabled could encourage risky behavior, and which are not required to complete the task...Companies should therefore assess which general functions and capabilities will be enabled or disabled for its workers based on its general business practices, industry requirements, and regulatory compliance needs... This paper will quantify an approach to identifying the most appropriate policies in various situations, and look at their impact both on the end user and the business.”





Contents

Introduction4

Defining Mobile Worker Smart Phone Policies.....4

Policy Impact Statement.....4

Determining Requirements.....6

Company Specific Requirements6

User Class Specific Requirements7

Some Impact Guidelines8

 Green level 8

 Yellow Level 9

 Red Level 10

How to Use this Guide 11

Policy “Groupings” 11

Logon and Authentication and Default Setup 11

Preventing Unauthorized Use..... 12

Data Protection and Encryption..... 12

Application Loading and Control..... 12

Malicious Code and User Action Limitation 12

Managing Network Access and Connectivity..... 12

Messaging and Collaboration functionality 12

Web Access Control..... 12

Peripheral Enablement (e.g., Cameras, Bluetooth, SD card)..... 13

Media Access..... 13

Policy Setting Recommendations..... 13

Logon and Authentication and Default Setup 13

 Figure 1: Logon and Authentication and Default Setup Group - Classification Where Policies
 Must First Be Changed From Default..... 15

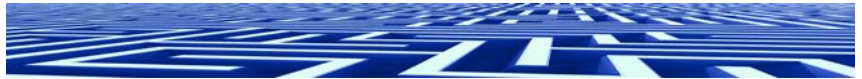
Preventing Unauthorized Use..... 16





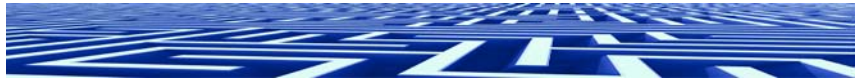
A Practical Guide to Deploying BlackBerry Polices

Figure 2: Preventing Unauthorized Use - Classification Where Policies Must First Be Changed From Default.....	17
<i>Data Protection and Encryption</i>	17
Figure 3: Preventing Unauthorized Use - Classification Where Policies Must First Be Changed From Default.....	19
<i>Application Loading and Control</i>	19
Figure 4: Application Loading and Control - Classification Where Policies Must First Be Changed From Default	20
<i>Malicious Code and User Action Limitation</i>	21
Figure 5: Malicious Code and User Action Limitation - Classification Where Policies Must First Be Changed From Default.....	22
<i>Managing Network Access and Connectivity</i>	22
Figure 6: Managing Network Access and Connectivity - Classification Where Policies Must First Be Changed From Default.....	23
<i>Messaging and Collaboration Functionality</i>	24
Figure 7: Managing Network Access and Connectivity - Classification Where Policies Must First Be Changed From Default.....	25
<i>Web Access Control</i>	25
Figure 8: Web Access Control - Classification Where Policies Must First Be Changed From Default	26
<i>Peripheral Enablement (e.g., Cameras, Bluetooth, SD card)</i>	26
Figure 9: Peripheral Enablement - Classification Where Policies Must First Be Changed From Default	27
<i>Media Access</i>	27
Figure 10: Media Access - Classification Where Policies Must First Be Changed From Default	27
<i>Policy Group Settings Summary</i>	28
Figure 11: Total Number of Policies per Grouping and Classification Level Where They Are First Changed from the Default Value	28
Conclusions	28
<i>Disclaimer</i>	29
Appendix	30
<i>Selected Regulatory Requirements</i>	30
SARBANES-OXLEY ACT (US).....	30



A Practical Guide to Deploying BlackBerry Polices

GRAMM-LEACH-BLILEY ACT (US)	30
HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA) (US).....	30
FDA TITLE 21 (US)	30
EUROPEAN UNION DIRECTIVE (EU)	30
EURO-SOX (EU)	31
CALIFORNIA SENATE BILL 1386 (US).....	31
PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI) (US).....	31
PERSONAL INFORMATION PROTECTION & ELECTRONIC DOCUMENTS ACT (Canada) .	31
DATA PROTECTION ACT (UK).....	31



A Practical Guide to Deploying BlackBerry Polices

Introduction

Most organizations will benefit by effectively managing their mobile devices. Benefits include lower cost of operations, securing against leakage of corporate data assets, meeting regulatory guidelines, maximizing workforce efficiency and minimizing support costs. Specific industries and worker classes may have unique requirements against which companies must develop a comprehensive set of policies and procedures to effectively deploy and maintain mobile devices. This guide will address creating requirements for specific scenarios and then provide concrete recommendations on which BlackBerry policies should be set to meet the organization's management and security needs. The policies included in this guide are based on those available with BlackBerry Enterprise Server version 5, but should generally be applicable to other versions as well.

Defining Mobile Worker Smart Phone Policies

Smart phones have become essential tools for business. To maximize their benefits, companies should determine which features and functions are appropriate in the user's work environment, which capabilities if enabled could encourage risky behavior, and which are not required to complete the task. For instance, some device features geared towards the consumer usage model create limited or even potentially harmful business effects (e.g., cameras, media players, web surfing, texting). Enabling them may be beneficial to the user despite not being work required, but companies must evaluate appropriate policy on a risk/reward basis. Companies should therefore assess which general functions and capabilities will be enabled or disabled for its workers based on its general business practices, industry requirements, and regulatory compliance needs.

Many companies determine their own set of corporate standards concerning compliance that may either be an extension of existing government regulations, or may be an attempt to create their own internal standards when no clearly defined external regulatory requirements exist. It is not uncommon for companies to have a pre-defined set of policies they have established which are created to limit liability and create a standardized environment for all employees. However, not all workers in the organization are necessarily treated equally, and specific rules and exceptions based on defined classes of workers, device type, specific organizational roles, and/or level within the corporate hierarchy may modify these general policies and their enforcement on an exception basis. Organizations should therefore remain flexible in specifying and deploying policies, and should assume that there will be individual exceptions to many of the general policies.

Policy Impact Statement

Companies must evaluate their policy requirements based on the impact they will have on both the business and the end user. Different business entities based on size or industry may be concerned with setting different policies. And different classes of users may have



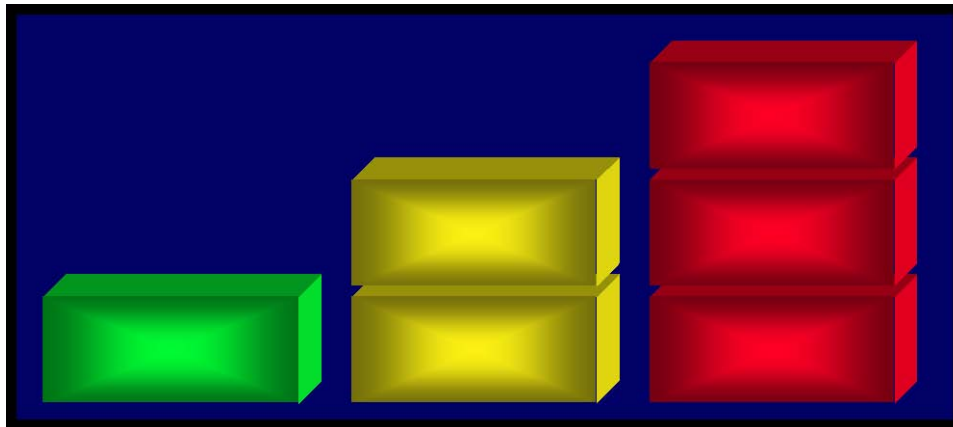
A Practical Guide to Deploying BlackBerry Polices

different desires and needs. Every policy choice will have an impact on the end user, as well as the organization. Full device lockdowns will maximize the end user impact by preventing users from accessing some functions of the device, but may offer increased amounts of protection to the business.

Each person, group and organization will see a different policy impact depending on job function, type of work done, regulatory situation, type of information accessible by users, etc. Risk/Reward considerations are important to judge what level of policy is acceptable in each situation. We recommend taking the approach of building a Policy Impact Statement that specifies what the impact will be on both the end user and the business entity when specific policies are enacted. From this analysis, companies can determine the requirements (on a scale of low to high) for implementation of various organizational and group policies.

This paper will quantify an approach to identifying the most appropriate policies in various situations, and look at their impact both on the end user and the business. We will also look at various job functions and generalize a set of policies for each based on certain assumptions about risk/reward and policy impact.

Our impact measurement will consist of a balance between the needs of the business and the wants/desires of the individual. For this evaluation, we will use the following ranking:



The three color coded levels represent a continuum from maximum openness of the device and end user control (Green) to maximum control by the enterprise or organization with limited control and access by the end user (Red). Red level policy settings will have the maximum impact on end users who may not appreciate the lack of personal flexibility. But Red also allows organizations to exert maximize control and achieve the highest level of management and security. Many company policies will fall somewhere in the middle.



A Practical Guide to Deploying BlackBerry Polices

Determining Requirements

While the needs of individual organizations will vary, we believe the following criteria need to be evaluated on a company by company basis in order to achieve a proper user and corporate impact balance. Organizations need to identify such key characteristics as:

- Company size (e.g., small, medium, large, distributed, centralized)
- Industry (e.g., manufacturing, retail, legal, financial services, healthcare)
- Whether subject to governmental regulations (e.g., HIPAA, SOX)
- Use with customer-sensitive data (e.g., credit cards, health records)
- User application requirements (e.g., email, corporate apps)
- Carrier data plan/expense management (e.g., voice, email, data, web access)
- Employee longevity/motivation (e.g., rapid turnover, easily move to competitor)
- Company furnished device or individually owned device
- Potential for loss of device

Each of these criteria will have an effect on the overall policy enforcement decision process, and will affect the level (e.g., green, red, something in between) of the general policies implemented.

Company Specific Requirements

Companies need to assess which policies are appropriate based upon their industry, size, regulatory requirements, mobile applications requirements, type of mobile workforce, etc. Appropriate policy setting will have an impact on the overall operations and efficiency of the organization. Policies may initially be evaluated on a company-wide basis, with some general company classes defined below. However, organizations should make certain modifications/exceptions to their general organization-wide policies based on the needs of the various classes of users within the company, which will be addressed in the next section.

Class 1 – Highly Regulated Industries – Industries such as financial services, health care, banking, insurance, retail and other companies that work with customer data and individual records are subject to a number of governmental regulations and significant penalties for non-compliance. These companies must use utmost care to prevent any data exposure, and often set policies that are highly restrictive. This class of company will generally engage in the most stringent review of user requirements and set the most stringent policies, including locking down features of the device (e.g., app loading, media player, web access) and severely restricting individual user control.

Class 2 – Larger Organizations – Enterprises generally have a high level of security in place to prevent the loss of sensitive corporate data and to limit the ability for outsiders to obtain access to corporate resources. These organizations generally set policies that make access and data discovery difficult, and often limit the type of user applications that can be utilized. However, enterprises may have a significant number of different user classes with diverse application needs (e.g., email, CRM, ERP) requiring multiple policies to meet individual needs rather than a single company-wide policy. Nevertheless, most policies are



A Practical Guide to Deploying BlackBerry Polices

set at relatively high levels to minimize risk, ensure corporate safety, and limit the amount of end user control over the device (e.g., only accessing email in a corporate-sanctioned way).

Class 3 – Medium Sized Enterprises – Mid-sized organizations are often less restrictive than large enterprises, allowing a reasonable amount of latitude in defining and implementing mobile device policies. This class of organization will generally set those policies that affect corporate access and data use to a medium level of restrictiveness, but may have individual policies modified for classes of workers (e.g., executives), and have relatively few restrictions on the personal use of the device.

Class 4 – Smaller Businesses – Smaller businesses generally implement a limited amount of policy level changes and often utilize the default settings inherent in deployed mobile infrastructure systems. Generally these organizations deploy the least restrictive level of policy and allow users the maximum amount of self control over their device.

User Class Specific Requirements

Company specific requirements are clearly important but may not be the only consideration in choosing which policy to implement for a given individual. Mobile workers in many organizations will fall into several different categories or user classes based on their function and level in the organization. And in addition to evaluating the impact based on specific organizational characteristics, companies should base any potential exceptions to general policies by identifying the needs of workers that fall into the following typical user classes:

Class 1 – High Level Executives – These individuals generally have access to highly sensitive corporate data files and communications as well as being subject to the most stringent regulatory compliance requirements. Policies for this class must include a high degree of data leakage prevention and device control. However, quite often this user class will not accept complete feature/function lockdown of the device, and will have the ability to influence or select certain features to be enabled. They may even have an ability to select alternative device models according to their own preference. Any policies governing this class will therefore have to take a balanced approach by maximizing corporate protection while allowing end user flexibility. This class will have the most exceptions implemented against general organizational policies, and can generally demand certain capabilities be implemented.

Class 2 – General Knowledge Workers – This class of workers is often involved in the day to day operations of the company and has access to sensitive corporate communications. Less impacted by regulatory issues than higher level executives, this class nevertheless requires a relatively high level of data leakage protection and device security. Access to functions like email, applications enablement, web and IM/texting are often required and should generally be allowed. Many companies also allow access to features like media player, camera and gaming. This class may have a significant number of individual exceptions to general organizational polices.



A Practical Guide to Deploying BlackBerry Policies

Class 3 – Administrative and Support Staff – This class of worker is generally involved in supporting executives and knowledge workers, and must have access to communications functions (email, texting) and certain types of applications involved in day to day operations. Most companies choose to control access to non-job specific functions of the device (i.e., web surfing, media player, camera) for this class of worker. This class of worker generally does not have the ability to obtain an individual exception to organizational policies.

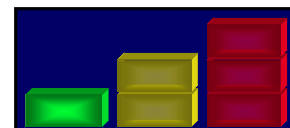
Class 4 – Production Workers – This class usually has the most restrictions applied to it as organizations generally lock out any capability that is not job-specific in nature. This class often has dedicated applications deployed, and may also include access to communications functions (i.e., email, IM). Most other functions/capabilities are governed by the corporate policies and few individual exceptions are implemented.

Class 5 – User Liable Device Owners – This is a relatively new user class that is based on the growing trend in which organizations allow their users to choose their own preferred device (within certain guidelines). This class is also often a subclass of the higher level (executive and knowledge worker) classes. It also represents the greatest challenge to organizations, as not all devices are equal to deploying business policies, even though many of the users in this class have access to very sensitive information. Companies must carefully evaluate offering User Liable devices based on the ability to manage and deploy corporate policies to those devices. Often, such devices will have only limited capabilities available to users to limit organizational exposure (i.e., limited access to email, and virtually no access to corporate apps). As the number and type of popular devices change, the need for individual exceptions to organizational policy will grow.

Some Impact Guidelines

Below are some specific guidelines that companies can follow to determine what level of control they should exercise. This is a suggested ranking and each organization should evaluate their specific needs on an individual basis. We will look at 5 key criteria: Company Characteristics, Industries, Access Types, Application Requirements and User Classes. We then suggest guidelines for each of the criteria for each level of control.

Green level



Company Characteristics: Primarily non-regulated industries and those industries that don't regularly work with personal or confidential materials. This level is also generally relevant for smaller organizations in the industries below that don't wish to supplement the default policies shipped with the device.



A Practical Guide to Deploying BlackBerry Polices

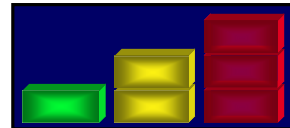
Industries: These industries might include construction, manufacturing, package delivery, real estate, facilities maintenance and some trades.

Access Types: Voice, email, messaging, limited Internet connectivity, limited or no organizational-specific applications.

Application Requirements: Primarily email based interactions. If any specific-use applications are required, they are primarily Web-based accessed through a browser. The user will have access to most features that are available within the standard device for both business and personal use.

User Classes: Generally applied to administration and support users and users with user liable devices that don't meet stricter company policy enforcement capabilities. In some cases, other classes may meet this level, but usually on an exception basis.

Yellow Level



Company Characteristics: Organizations that deal with sensitive company or client information that could be sensitive if disclosed. This includes company financial data, competitive information, and client directed interactions. This level may be relevant as a more secure environment than the one above for smaller organizations in the industries below. This level is generally applicable for medium to larger organizations and those that are divisions within enterprises who require access to corporate systems.

Industries: Education, maintenance and repair workers, retail clerks, tradesmen, knowledge workers, information technology, consultants, professional services

Access Types: Voice, email, messaging, customer contact information, personal information on clients and organizational information, access to corporate back office systems, special purpose applications, web browsing.

Application Requirements: Limiting organizational or industry-supplied applications to specific purposes, including limitations on use of personal applications to minimize organizational exposure to sensitive data loss. Users often require access to customer data and corporate applications (e.g., Exchange, Word, Excel, CRM, ERP). This may require purpose-build applications. Organizations should restrict some functions of the device and limit the ability to download new applications to protect sensitive data on the device. Restrictions to user control of the device (e.g., password, configuration) are generally applied.

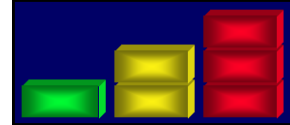
User Classes: General knowledge workers fall into this category, as do some higher level executives in unregulated industries or where data is not of a sensitive nature. Some



A Practical Guide to Deploying BlackBerry Polices

knowledge workers and executives may fit into this category by exception even within companies that generally would set higher level policies for their use.

Red Level



Company Characteristics: Companies that have real time data requirements and where information transmission in a time critical manner is imperative. These organizations are often public service entities, or workers within larger organizations that may need access to corporate applications, data and resources. This class applies to organizations that work with credit card information, financial transaction records, personally identifiable information, or corporate sensitive information and that must meet strict regulatory compliance and legal requirements. Many corporate executives often fall under this category.

Industries: Public utilities, public services (e.g., Fire, Police), health care, enterprise executives, financial services, accounting, legal services

Access Types: Voice, email (restricted to organizational infrastructure), limited messaging, limited app loading and use (restricted to organizational selection and loading), limited use of personal apps (e.g., media player, personal messaging) that may hinder or expose sensitive information, and may or may not allow web browsing depending on circumstances.

Application Requirements: Often includes purpose-built apps that are the cornerstone of the worker's productivity. Such dedicated workers are restricted from the more personal use capabilities of the device, which they can access by exception only (e.g., web browsing, music, camera, peripheral support). Most devices in this class of user are heavily controlled by the organization to protect against any sensitive and potentially legally actionable data losses. While some organizational special purpose apps are included, the scope and access capability are closely managed. This group generally has no user control of device set-up, modification and working parameters.

User Classes: This level is generally reserved for classes of workers dealing with highly sensitive data and/or dedicated production workers who need to have access limited to specific functions. Support and Administration classes may also fall into this category, as well as certain knowledge workers. User liable devices with minimal policy enforcement capabilities also fall into this category.



How to Use this Guide

Below we identify 10 policy area groupings that include generally related policies, and then within each grouping, three policy enforcement levels (green, yellow and red) that represent increasingly more stringent levels of organizational control and/or meet particular needs. Most companies will likely implement the suggested policy settings primarily from the green or yellow group, with organizations implementing the red policy settings to meet the special or more stringent control requirements of certain regulated industries or organizational classes. For each color coded setting, we provide a suggested setting point for that policy (either the default value, or an alternative).

As a general rule, the green policy settings define what we believe is a minimum setting, enabling maximum control by the user. Control shifts increasingly towards the organization as policy settings in the yellow and red levels are implemented. Companies with a specific general policy level setting may need to modify that setting for a particular class of users. Therefore, although an organization may choose a general policy setting, individual exceptions for specific classes of users may require a change to that setting (either higher or lower), and companies should evaluate users based on both general policy and class before a final setting is determined.

Although many organizations can likely accept the recommended settings provided for many policies, they should nevertheless evaluate the suggested settings to see if they meet the particular needs of the organization. The policy settings identified by the three color codes are suggestions and/or starting points and companies should look at each policy keeping its own unique needs in mind, and then accept or modify them accordingly.

Below we provide details on the individual policy groupings, and then provide recommended settings based on our color-coded criteria described earlier.

Policy “Groupings”

Many related policies can be grouped together to achieve a specific purpose or set a specific control point. These policy groupings can then be set at a specific level to achieve a broad-based level of management and/or protection for the organization. While the groupings are somewhat subjective, below are 10 key areas where we believe grouping policies can be effective. Further, these groupings allow the organization to assess the level of importance or criticality to the business in enforcing these policies, by assigning a relative value to them based on the organization’s profile (e.g., size of business, industry, regulatory and statutory obligations, etc.).

Logon and Authentication and Default Setup

This grouping is related to the need for passwords and authentication on the device. The complexity level of the password is relevant as more complex passwords are harder to guess and therefore offer more security should the device be lost or stolen. Further, timeouts



A Practical Guide to Deploying BlackBerry Polices

provide an ability to lock a device after it remains idle. Finally, this group also sets up various end user preferences, defaults and functions related to the device and desktop interactions.

Preventing Unauthorized Use

This grouping is related to blocking unauthorized users from gaining access to the device and discovering potentially sensitive data contained therein. It includes owner information and lockout settings which are critical to protect the data contents of the device.

Data Protection and Encryption

This grouping involves policies which protect individual files and data stored on the device. It involves policies which enforce private key storage for encryption, content protection strength, encryption settings/strength, and device wiping. These policies are necessary to secure the device, set the device for compliance with various standards, and clear the device of sensitive information should it be lost or stolen.

Application Loading and Control

This grouping defines the types of applications that can be loaded onto the device, as well as how and when applications may be used. These policies establish how users interact with the device and how the organization controls that interaction.

Malicious Code and User Action Limitation

This grouping provides control of applications to prevent loading unsafe or malicious applications to the device. It further defines the actions and limitations of the browser, to protect the device from malicious attack.

Managing Network Access and Connectivity

This grouping involves policies that define how and when the device connects, what location information is provided, and SIM-related functions and capabilities such as when and how calls are made. These policies also define how often and what contents of the device are synchronized to protect the integrity of the device and its data.

Messaging and Collaboration functionality

This grouping defines the functions and capabilities of the device in the various messaging functions it enables., including SMS, MSM and PIN to PIN messaging, the messaging encryption key management and the duration of time between synchronization.

Web Access Control

This policy grouping controls the functionality of the browser and Internet access, including when it can be used, what functions of the browser are available, what types of content can be viewed and how attachments may be handled. This policy grouping is critical to determining the device's Internet capabilities for general browsing as well as company Internet-based applications.



A Practical Guide to Deploying BlackBerry Polices

Peripheral Enablement (e.g., Cameras, Bluetooth, SD card)

This grouping determines how peripherals, particularly Bluetooth enabled peripherals, will connect and interact with the device. Further, it determines how add-on memory functions, as well as camera functionality. This grouping determines the ability of the device to utilize external and internal peripheral resources and provide a way for organizations to prevent user interactions with peripherals.

Media Access

This grouping provides policies to determine how media on the device will be accessed and what functionality users will have enabled.

We suggest companies evaluate the importance for each policy group, and individual policies in the groupings, based on their needs. This information will then be used to decide on the appropriate policies to set.

Policy Setting Recommendations

Below, within each of the groupings identified above, we indicate a recommended policy setting for each color coded level (green, yellow, red) representing the levels from maximum end user control to maximum organizational control. There are in excess of 450 individual BlackBerry Enterprise Server polices that can be set, but we have included only the most popular policy settings in this guide. Please consult The BlackBerry Policy Reference Guide for greater detail on the policies briefly described below, as well as additional policies available for the BlackBerry.

Logon and Authentication and Default Setup

- **Password Required**

This rule specifies whether a user must configure a password on a BlackBerry® device.

- We recommend the following settings:

Green – True **Yellow** – True **Red** - True

- **User Can Disable Password**

This rule specifies whether a user can turn off a BlackBerry® device password.

- We recommend the following settings:

Green – True **Yellow** – False **Red** - False

- **Force Lock When Holstered**

This rule specifies whether a BlackBerry® device locks when a user inserts it in the holster.

- We recommend the following settings:

Green – False **Yellow** – True **Red** - True



A Practical Guide to Deploying BlackBerry Polices

- **Set Owner Info**

This rule specifies the owner information that appears on a BlackBerry® device.

- We recommend the following settings:

Green – Default = Not Required **Yellow** – Required **Red** - Required

- **Maximum Password Age**

This rule specifies the number of days before a BlackBerry® device password expires and a user must set a new password. The permitted range is 0 through 65,535.

- We recommend the following settings:

Green – 180 Days **Yellow** – 60 Days **Red** – 30 Days

- **Maximum Password History**

This rule specifies the maximum number of previous passwords that a BlackBerry® device checks new passwords against to prevent a user from reusing previous passwords.

- We recommend the following settings:

Green – Default = 0 **Yellow** – 6 **Red** – 6

- **Minimum Password Length**

This rule specifies the minimum number of characters that are required for a BlackBerry® device password. The permitted range is 4 through 14 characters. The maximum password length, which this rule does not control, is 32 characters.

- We recommend the following settings:

Green – 4 **Yellow** – 6 **Red** – 8

- **Suppress Password Echo**

This rule specifies whether, after a given number of incorrect password attempts, the characters that a user types in the Password dialog box appear on the screen.

- We recommend the following settings:

Green – Default = True **Yellow** – Default = True **Red** – False

- **Lock Owner Info**

This rule specifies whether a user can change the owner information for a BlackBerry® device. You can lock the Information field, the Name field, or both fields.

Green – Default = No Restriction **Yellow** – Lock both Name and Information text **Red** – Lock both Name and Information text

- **Set Maximum Password Attempts**

This rule specifies the number of password attempts that a user can make before a BlackBerry® device erases all of the application data. The permitted range is 3 through 10 attempts.

- We recommend the following settings:

Green – Default = 10 **Yellow** – 7 **Red** – 5



A Practical Guide to Deploying BlackBerry Polices

- **Set Password Timeout**
 This rule specifies the number of minutes of inactivity before the security timeout occurs and a BlackBerry® device user must type the password to unlock the BlackBerry device.

 - We recommend the following settings:
 - Green** – 30 Minutes
 - Yellow** – 15 Minutes
 - Red** – 5 Minutes

- **Password Pattern Checks**
 This rule specifies whether to verify that a BlackBerry® device password matches certain character pattern requirements.

 - We recommend the following settings:
 - Green** – Default = No Restrictions
 - Yellow** – At least 1 alpha and 1 numeric character
 - Red** – At least 1 alpha, 1 numeric, and 1 special character.

Figure 1: Logon and Authentication and Default Setup Group - Classification Where Policies Must First Be Changed From Default

<i>Logon and Authentication and Default Setup</i>	Green	Yellow	Red
Password Required	<input checked="" type="checkbox"/>		
User Can Disable Password		<input checked="" type="checkbox"/>	
Force Lock When Holstered		<input checked="" type="checkbox"/>	
Set Owner Info		<input checked="" type="checkbox"/>	
Maximum Password Age	<input checked="" type="checkbox"/>		
Maximum Password History		<input checked="" type="checkbox"/>	
Minimum Password Length	<input checked="" type="checkbox"/>		
Suppress Password Echo			<input checked="" type="checkbox"/>
Lock Owner Info		<input checked="" type="checkbox"/>	
Set Maximum Password Attempts		<input checked="" type="checkbox"/>	
Set Password Timeout	<input checked="" type="checkbox"/>		
Password Pattern Checks		<input checked="" type="checkbox"/>	



Preventing Unauthorized Use

- **Maximum Security Timeout**

This rule specifies the maximum time (in minutes) that a BlackBerry® device user can specify as the security timeout value. The security timeout value is the number of minutes of inactivity before the device locks. The permitted range is 10 through 480 minutes.

- We recommend the following settings:

Green – 60 Minutes **Yellow** – 15 Minutes **Red** – 5 Minutes

- **User Can Change Timeout**

This rule specifies whether a BlackBerry® device user can override the security timeout value.

- We recommend the following settings:

Green – Default = True **Yellow** – True **Red** – False

- **Remote Wipe Reset to Factory Defaults**

This rule specifies whether a BlackBerry® device resets to the default settings when it receives the Erase Data and Disable Handheld IT administration command over a wireless network.

- We recommend the following settings:

Green – Default = False **Yellow** – True **Red** – True

- **Allow Outgoing Call When Locked**

This rule specifies whether users can place calls while a BlackBerry® device is locked.

- We recommend the following settings:

Green – True **Yellow** – True **Red** – Default = False

- **Enable Long-Term Timeout**

This rule specifies whether a BlackBerry® device locks after a predefined period of time, regardless of user activity.

- We recommend the following settings:

Green – Default = False **Yellow** – Default = False **Red** – True



A Practical Guide to Deploying BlackBerry Polices

Figure 2: Preventing Unauthorized Use - Classification Where Policies Must First Be Changed From Default

<i>Preventing Unauthorized Use</i>	Green	Yellow	Red
Maximum Security Timeout	<input checked="" type="checkbox"/>		
User Can Change Timeout			<input checked="" type="checkbox"/>
Remote Wipe Reset to Factory Defaults		<input checked="" type="checkbox"/>	
Allow Outgoing Call When Locked			<input checked="" type="checkbox"/>
Enable Long-Term Timeout			<input checked="" type="checkbox"/>

Data Protection and Encryption

- Content Protection Strength**
 This rule specifies the cryptography strength that a BlackBerry® device uses to encrypt content that it receives while it is locked. When you specify a value, the content protection feature is turned on.
 - We recommend the following settings:
Green – Strong **Yellow** – Stronger **Red** – Strongest
- Disable Address Book Transfer**
 This rule specifies whether to prevent a BlackBerry® device from exchanging address book data with a supported Bluetooth® enabled device.
 - We recommend the following settings:
Green – Default = False **Yellow** – True **Red** – True
- Disable File Transfer**
 This rule specifies whether to prevent a BlackBerry® device from exchanging files with supported Bluetooth® OBEX devices.
 - We recommend the following settings:
Green – Default = False **Yellow** – True **Red** – True
- Allow Screen Shot Capture**
 This rule specifies whether a BlackBerry® device permits applications, including third-party applications, to take screen shots.
 - We recommend the following settings:
Green – Default = True **Yellow** – False **Red** – False
- Require LED Connection Indicator**
 This rule specifies whether the LED must flash when a BlackBerry® device is connected to a Bluetooth® enabled device.



A Practical Guide to Deploying BlackBerry Polices

- We recommend the following settings:
Green – True **Yellow** – True **Red** – True
- **Disable Phone Call Log Wireless Synchronization**
This rule specifies whether wireless data synchronization for call logs is turned off.
 - We recommend the following settings:
Green – Default = False **Yellow** – Default = False **Red** – True
- **Disable Memopad Wireless Synchronization**
This rule specifies whether wireless data synchronization for memos is turned off.
 - We recommend the following settings:
Green – Default = False **Yellow** – Default = False **Red** – True
- **Disable Organizer Data Access Applications**
This rule specifies whether an application can access the BlackBerry® device PIM APIs, which control access to the user's personal information on the BlackBerry device, such as the address book.
 - We recommend the following settings:
Green – Default = Allowed **Yellow** – Default = Allowed **Red** – Not Allowed
- **Disable Wi-Fi Direct Access to BlackBerry Enterprise Server**
This rule specifies whether a BlackBerry® device can connect to the BlackBerry® Enterprise Server using a Wi-Fi® connection.
 - We recommend the following settings:
Green – Default=No **Yellow** – Default=No **Red** – Yes
- **Disable Wireless Bypass**
This rule specifies whether a BlackBerry® device uses wireless bypass using Bluetooth® technology
 - We recommend the following settings:
Green – Default = True **Yellow** – False **Red** – False
- **Disable Wi-Fi IT**
This rule specifies whether a user can access a Wi-Fi® network from a Wi-Fi enabled BlackBerry® device.
 - We recommend the following settings:
Green – Default = No **Yellow** – Default = No **Red** – Yes
- **Keep Message Duration**
This rule specifies the maximum time (in days) that a BlackBerry® device keeps messages. The permitted range is -1 through 180 days.
 - We recommend the following settings:
Green – Default = -1 to Keep Messages Indefinitely **Yellow** – 90 Days **Red** – 30 Days



A Practical Guide to Deploying BlackBerry Polices

Figure 3: Preventing Unauthorized Use - Classification Where Policies Must First Be Changed From Default

<i>Data Protection and Encryption</i>	Green	Yellow	Red
Content Protection Strength	<input checked="" type="checkbox"/>		
Disable Address Book Transfer		<input checked="" type="checkbox"/>	
Disable File Transfer		<input checked="" type="checkbox"/>	
Allow Screen Shot Capture		<input checked="" type="checkbox"/>	
Require LED Connection Indicator	<input checked="" type="checkbox"/>		
Disable Phone Call Log Wireless Synchroniz			<input checked="" type="checkbox"/>
Disable Memopad Wireless Synchroniz			<input checked="" type="checkbox"/>
Disable Organizer Data Access Apps			<input checked="" type="checkbox"/>
Disable Wi-Fi Direct Access to BES			<input checked="" type="checkbox"/>
Disable Wireless Bypass		<input checked="" type="checkbox"/>	
Disable Wi-Fi IT			<input checked="" type="checkbox"/>
Keep Message Duration		<input checked="" type="checkbox"/>	

Application Loading and Control

- Allow Application Download Services**
 This rule specifies whether application download service icons appear on a BlackBerry® device when the wireless service provider assigns a service to a BlackBerry device and the appropriate service books are present on the BlackBerry device.
 - We recommend the following settings:
Green – Default = True **Yellow** – False **Red** – False
- Disallow Third Party Application Downloads**
 This rule specifies whether a user can install an application that the Research In Motion® signing authority system has not digitally signed on a BlackBerry® device.
 - We recommend the following settings:
Green – False **Yellow** – Default = True **Red** – Default = True
- Disable Public Photo Sharing Applications**
 This rule specifies whether to prevent a BlackBerry® device user from uploading pictures to the Internet using public photo sharing applications.



A Practical Guide to Deploying BlackBerry Polices

- We recommend the following settings:
Green – Default = False Yellow – True Red – True

- **Disable Public Social Networking Applications**
 This rule specifies whether a user can install public social networking applications on a BlackBerry® device to access public social networking services (for example, Facebook®).
 - We recommend the following settings:
Green – Default = False Yellow – Default = False Red – True

- **Allow Third Party Apps to Use Serial Port**
 This rule specifies whether third-party applications can use the serial port, IrDA® port, or USB port on a BlackBerry® device.
 - We recommend the following settings:
Green – Default = True Yellow – False Red – False

- **Disable BlackBerry App World**
 This rule specifies whether the BlackBerry App World™ application is turned off on the BlackBerry® device
 - We recommend the following settings:
Green – Default=False Yellow – Default=False Red – True

- **Disable Application Center**
 This rule specifies whether to prevent the application center from running on a BlackBerry® device.
 - We recommend the following settings:
Green – Default = False Yellow – Default = False Red – True

Figure 4: Application Loading and Control - Classification Where Policies Must First Be Changed From Default

<i>Application Loading and Control</i>	Green	Yellow	Red
Allow Application Download Services		<input checked="" type="checkbox"/>	
Disallow Third Party App Downloads		<input checked="" type="checkbox"/>	
Disable Public Photo Sharing Applications		<input checked="" type="checkbox"/>	
Disable Public Social Networking Apps			<input checked="" type="checkbox"/>
Allow Third Party Apps to Use Serial Port		<input checked="" type="checkbox"/>	
Disable BlackBerry App World			<input checked="" type="checkbox"/>
Disable Application Center			<input checked="" type="checkbox"/>



Malicious Code and User Action Limitation

- **Disable Serial Port Profile**
This rule specifies whether a BlackBerry® device can use the Bluetooth® SPP.
 - We recommend the following settings:
Green – True **Yellow** – True **Red** – True
- **Disallow Device User Requested Upgrade**
This rule specifies whether to prevent a BlackBerry® device user from requesting available updates for the BlackBerry® Device Software over the wireless network.
 - We recommend the following settings:
Green – Default = False **Yellow** – Default = False **Red** – True
- **Disallow Device User Requested Rollback**
This rule specifies whether to prevent a BlackBerry® device user from returning to a previous version of the BlackBerry® Device Software after a previously successful update of the BlackBerry Device Software over the wireless network.
 - We recommend the following settings:
Green – Default = False **Yellow** – True **Red** – True
- **Disable Desktop Connectivity**
This rule specifies whether to prevent a BlackBerry® device from using Bluetooth® technology to connect to the BlackBerry® Desktop Software.
 - We recommend the following settings:
Green – False **Yellow** – Default = True **Red** – Default = True
- **Allow Non Enterprise Upgrade**
This rule specifies whether to permit Research In Motion or a wireless service provider to request that a BlackBerry® device download updates to the BlackBerry® Device Software over the wireless network.
 - We recommend the following settings:
Green – True **Yellow** – Default = False **Red** – Default = False
- **Attachment Viewing**
This rule specifies whether a BlackBerry® device user can view supported attachments in messages and calendar entries.
 - We recommend the following settings:
Green – Default = True **Yellow** – Default = True **Red** – False



A Practical Guide to Deploying BlackBerry Policies

Figure 5: Malicious Code and User Action Limitation - Classification Where Policies Must First Be Changed From Default

<i>Malicious Code and User Action Limitation</i>	Green	Yellow	Red
Disable Serial Port Profile	<input checked="" type="checkbox"/>		
Disallow Device User Requested Upgrade			<input checked="" type="checkbox"/>
Disallow Device User Requested Rollback		<input checked="" type="checkbox"/>	
Disable Desktop Connectivity	<input checked="" type="checkbox"/>		
Allow Non Enterprise Upgrade		<input checked="" type="checkbox"/>	
Attachment Viewing			<input checked="" type="checkbox"/>

Managing Network Access and Connectivity

- Disable Discoverable Mode**
 This rule specifies whether to prevent BlackBerry® device users from making their BlackBerry device discoverable. A BlackBerry device that is discoverable can be found by other Bluetooth® enabled devices within range of the BlackBerry device.
 - We recommend the following settings:
Green – False **Yellow** – False **Red** – False
- Wi-Fi Allow Handheld Changes**
 This rule specifies whether users can change all Wi-Fi® policy rules on their BlackBerry® devices.
 - We recommend the following settings:
Green – Default=Yes **Yellow** – No **Red** – No
- Enable Enterprise Location Tracking**
 This rule specifies whether a BlackBerry® device can use the GPS feature to report its location to the BlackBerry® Enterprise Server regularly. A BlackBerry device user must click Yes when prompted to permit location tracking on a BlackBerry device.
 - We recommend the following settings:
Green – Default = False **Yellow** – True **Red** – True
- Allow Public WLM Services**
 This rule specifies whether a user can use Windows Live™ Messenger on a BlackBerry® device.
 - We recommend the following settings:
Green – Default = True **Yellow** – False **Red** – False



A Practical Guide to Deploying BlackBerry Polices

- **Disable Forwarding Between Services**

This rule specifies whether to prevent a BlackBerry® device user from forwarding or replying to a message on a BlackBerry device using an email account or messaging service that is associated with a BlackBerry® Enterprise Server or BlackBerry® Internet Service that is different from the service that delivered the original message. Use this rule to prevent forwarding or replying to a PIN message with an email message, or replying to an email message with a PIN message.

- We recommend the following settings:

Green – Default = False **Yellow** – True **Red** – True

- **Disable Dial-Up Networking**

This rule specifies whether to prevent a BlackBerry® device from using the Bluetooth® DUN profile

- We recommend the following settings:

Green – Default = False **Yellow** – True **Red** – True

- **Allow Split-Pipe Connections**

This rule specifies whether applications, including third-party applications, can open internal and external connections on a BlackBerry® device simultaneously. Opening internal and external connections simultaneously might present a security issue because applications can collect data from inside the firewall and send it outside the firewall without any auditing.

- We recommend the following settings:

Green – Default = False **Yellow** – Default = False **Red** – True

Figure 6: Managing Network Access and Connectivity - Classification Where Policies Must First Be Changed From Default

Managing Network Access and Connectivity	Green	Yellow	Red
Disable Discoverable Mode	<input checked="" type="checkbox"/>		
Wi-Fi Allow Handheld Changes		<input checked="" type="checkbox"/>	
Enable Enterprise Location Tracking		<input checked="" type="checkbox"/>	
Allow Public WLM Services		<input checked="" type="checkbox"/>	
Disable Forwarding Between Services		<input checked="" type="checkbox"/>	
Disable Dial-Up Networking		<input checked="" type="checkbox"/>	
Allow Split-Pipe Connections			<input checked="" type="checkbox"/>



Messaging and Collaboration Functionality

- **Allow Peer-to-Peer Messages**

This rule specifies whether a user can send PIN messages.

- We recommend the following settings:

Green – Default = True **Yellow** – Default = True **Red** – False

- **Allow Public AIM Services**

This rule specifies whether a user can use AOL® Instant Messenger™ (AIM® service) on a BlackBerry® device.

- We recommend the following settings:

Green – Default = True **Yellow** – False **Red** – False

- **Allow Public ICQ Services**

This rule specifies whether a user can use ICQ® on a BlackBerry® device.

- We recommend the following settings:

Green – Default = True **Yellow** – False **Red** – False

- **Allow SMS**

This rule specifies whether a user can send SMS text messages.

- We recommend the following settings:

Green – Default = True **Yellow** – Default = True **Red** – False

- **Disable SMS Messages Wireless Synchronization**

This rule specifies whether wireless data synchronization for SMS text messages is turned off.

- We recommend the following settings:

Green – Default = True **Yellow** – Default = True **Red** – False

- **Allow Public Google Talk Services**

This rule specifies whether a user can use Google Talk™ on a BlackBerry® device.

- We recommend the following settings:

Green – Default = True **Yellow** – False **Red** – False

- **Allow Public IM Services**

This rule specifies whether a user can use public instant messaging applications for BlackBerry® devices.

- We recommend the following settings:

Green – Default = True **Yellow** – False **Red** – False

- **Disable BlackBerry Messenger**

This rule specifies whether BlackBerry® Messenger is turned off.

- We recommend the following settings:

Green – Default = False **Yellow** – Default = False **Red** – True



A Practical Guide to Deploying BlackBerry Polices

- **Disable MMS**
This rule specifies whether a BlackBerry® device user can send and receive MMS messages.
 - We recommend the following settings:
Green – Default = False **Yellow** – True **Red** – True

Figure 7: Managing Network Access and Connectivity - Classification Where Policies Must First Be Changed From Default

<i>Messaging and Collaboration Functionality</i>	Green	Yellow	Red
Allow Peer-to-Peer Messages			<input checked="" type="checkbox"/>
Allow Public AIM Services		<input checked="" type="checkbox"/>	
Allow Public ICQ Services		<input checked="" type="checkbox"/>	
Allow SMS			<input checked="" type="checkbox"/>
Disable SMS Messages Wireless Synch			<input checked="" type="checkbox"/>
Allow Public Google Talk Services		<input checked="" type="checkbox"/>	
Allow Public IM Services		<input checked="" type="checkbox"/>	
Disable BlackBerry Messenger			<input checked="" type="checkbox"/>
Disable MMS		<input checked="" type="checkbox"/>	

Web Access Control

- **Allow IBS Browser**
This rule specifies whether a separate icon appears on a BlackBerry® device if the appropriate service books are present for BlackBerry Internet Service Browsing.
 - We recommend the following settings:
Green – Default = True **Yellow** – False **Red** – False
- **Enable WAP Config.**
This rule specifies whether a separate icon appears on a BlackBerry® device if the appropriate service books are present for the WAP Browser.
 - We recommend the following settings:
Green – Default = True **Yellow** – False **Red** – False
- **Disable JavaScript in Browser**
This rule specifies whether the BlackBerry® Browser can run JavaScript®.
 - We recommend the following settings:
Green – Default = False **Yellow** – Default = False **Red** – True



Figure 8: Web Access Control - Classification Where Policies Must First Be Changed From Default

Web Access Control	Green	Yellow	Red
Allow IBS Browser		<input checked="" type="checkbox"/>	
Enable WAP Config		<input checked="" type="checkbox"/>	
Disable JavaScript in Browser			<input checked="" type="checkbox"/>

Peripheral Enablement (e.g., Cameras, Bluetooth, SD card)

- Disable USB Mass Storage**
 This rule specifies whether USB mass storage is turned on. If you change this rule to True, a BlackBerry® device cannot access an external file system that is connected to the USB port.

 - We recommend the following settings:
Green – Default=False **Yellow** – Default=False **Red** – True
- Require Password for Discoverable Mode**
 This rule specifies whether a user must type the BlackBerry® device password before a BlackBerry device can be discovered by Bluetooth® enabled devices.

 - We recommend the following settings:
Green – Default = False **Yellow** – Default = False **Red** – True
- Require Password for Enabling Bluetooth Support**
 This rule specifies whether a user must type the BlackBerry® device password to turn on Bluetooth® technology.

 - We recommend the following settings:
Green – Default = False **Yellow** – Default = False **Red** – True
- Disable Bluetooth**
 This rule specifies whether support for Bluetooth® technology on a BlackBerry® device is turned off.

 - We recommend the following settings:
Green – Default = False **Yellow** – Default = False **Red** – True
- Disable Photo Camera**
 This rule specifies whether the camera is available on a BlackBerry® device.

 - We recommend the following settings:
Green – Default = False **Yellow** – Default = False **Red** – True



A Practical Guide to Deploying BlackBerry Policies

- **Disable Video Camera**

This rule specifies whether the video camera feature on a BlackBerry® device is turned on.

- We recommend the following settings:

Green – Default = False **Yellow** – Default = False **Red** – True

Figure 9: Peripheral Enablement - Classification Where Policies Must First Be Changed From Default

<i>Peripheral Enablement</i>	Green	Yellow	Red
Disable USB Mass Storage			<input checked="" type="checkbox"/>
Require Password for Discoverable Mode			<input checked="" type="checkbox"/>
Require Password for Enabling Bluetooth			<input checked="" type="checkbox"/>
Disable Bluetooth			<input checked="" type="checkbox"/>
Disable Photo Camera			<input checked="" type="checkbox"/>
Disable Video Camera			<input checked="" type="checkbox"/>

Media Access

- **External File System Encryption Level**

This rule specifies the level of encryption that a BlackBerry® device uses to encrypt files that it stores on an external file system, such as an external memory device.

- We recommend the following settings:

Green – Not Required **Yellow** – Required **Red** – Required

- **Disable External Memory**

This rule specifies whether to prevent a BlackBerry® device user from accessing the media card on a supported BlackBerry device.

- We recommend the following settings:

Green – Default = False **Yellow** – Default = False **Red** – True

Figure 10: Media Access - Classification Where Policies Must First Be Changed From Default

<i>Media Access</i>	Green	Yellow	Red
External File System Encryption Level		<input checked="" type="checkbox"/>	
Disable External Memory			<input checked="" type="checkbox"/>



Policy Group Settings Summary

Below we provide a summary chart that indicates how many policies are discussed within each of the policy groups, as well as the number of policies that are first changed from the default value in their respective color-coded area.

Figure 11: Total Number of Policies per Grouping and Classification Level Where They Are First Changed from the Default Value

<i>Total Policies Per Area and Level</i>	Green	Yellow	Red
Logon and Authentication and Default Setup	4	7	1
Preventing Unauthorized Use	1	1	3
Data Protection and Encryption	2	5	5
Application Loading and Control		4	3
Malicious Code and User Action Limitation	2	2	2
Managing Network Access and Connectivity	1	5	1
Messaging and Collaboration Functionality		5	4
Web Access Control		2	1
Peripheral Enablement			6
Media Access		1	1
Total Number of Policies	10	32	27

Conclusions

This guide has provided specific recommendations to secure mobile devices that should cover most organizations in meeting their regulatory compliance and special situation requirements. These recommendations included defining the general security requirements of mobile workers and then mapping specific BES policies to enable and enforce those requirements. However, there may be exceptions not covered within this paper. Please consult with a knowledgeable security specialist if your situation requires customization or modification of the above recommended deployment scenarios.



A Practical Guide to Deploying BlackBerry Polices

Disclaimer

The information contained in this document is provided in good faith, and every reasonable effort is made to ensure that it is correct and up to date. Although the information provided in this document is obtained or compiled from sources we believe to be reliable, we cannot and do not guarantee the accuracy, validity, timeliness, completeness or reliability of any information or data made available to you or its suitability for any particular purpose. The information in this document is provided without warranty and may contain inaccuracies or typographical errors.

J.Gold Associates, LLC. does not warrant the accuracy and completeness of the information in this document. The information contained in this document may be changed or updated at any time without notice. Accordingly, this information is provided 'as is' without warranty of any kind. J.Gold Associates, LLC excludes all warranties, either express or implied (including, but not limited to any implied warranties of merchantability, fitness for a particular purpose, satisfactory quality or freedom from hidden defects). Any person relying on any of the information contained in this document or making any use of the information contained herein, shall do so at its own risk.

To the fullest extent permitted by the applicable law, J.Gold Associates, LLC hereby disclaims any liability and in no event shall J.Gold Associates, LLC be liable for any damage including, without limitation, direct, indirect or consequential damages including loss of revenue, loss of profit, loss of opportunity or other loss arising from the use of or the inability to use the information contained in this document including damages arising from inaccuracies, omissions or errors.



Appendix

Selected Regulatory Requirements

Nearly all companies are required to meet governmental oversight and regulatory compliance pertaining to both corporate and customer/individual data. Further, specific industries have particular sets of requirements (e.g., HIPAA in Healthcare, PCI in retail) and new regulations are being enacted (e.g., CA, MA state regulations in the US). Below we briefly highlight several of the major worldwide regulations that companies must adhere to if they are to establish a defense against regulatory noncompliance. These regulations should be considered by companies when implementing specific BlackBerry policies so that the organization effectively meets its compliance requirements.

SARBANES-OXLEY ACT (US)

- Intent – The protection of data related to financial reporting within public companies
- Affected – Applicable to all public companies in all industries
- Enforcement and Penalties – Both Civil and Criminal enforcement and penalties are possible

GRAMM-LEACH-BLILEY ACT (US)

- Intent – Protection of all private data within the financial industry
- Affected – The Financial Services and Banking industries, and related governmental agencies.
- Enforcement and Penalties – Significant fines and possible criminal prosecution

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA) (US)

- Intent – the protection of all personal healthcare records and related information
- Affected – All industries and organizations doing business in the US
- Enforcement and Penalties – Both civil and criminal penalties

FDA TITLE 21 (US)

- Intent – Criteria to establish trustworthy electronic records and signatures
- Affected - All Pharmaceutical and other FDA-regulated industries doing business in the US
- Enforcement and Penalties – Both criminal and civil prosecutions and penalties

EUROPEAN UNION DIRECTIVE (EU)

- Intent – To require the general protection for an individual's private information
- Affected – All organizations and institutions in the EU
- Enforcement and Penalties – Determined on case by case basis



A Practical Guide to Deploying BlackBerry Polices

EURO-SOX (EU)

- Intent - Protection of all sensitive data related to the public financial reporting process
- Affected – All Banking and Financial services companies in EU
- Enforcement and Penalties - Criminal and civil prosecution with significant potential fines

CALIFORNIA SENATE BILL 1386 (US)

- Intent - The protection of individual private information for all residents of CA
- Affected – any organization doing business in CA or with employees in CA
- Enforcement and Penalties - Fines

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI) (US)

- Intent - The protection of all payment data and consumer information during processing, transmission, and storage of financial details
- Affected – all transactions by MasterCard, Visa and other payment cards
- Enforcement and Penalties - Significant fines and loss of payment card capabilities

PERSONAL INFORMATION PROTECTION & ELECTRONIC DOCUMENTS ACT (Canada)

- Intent – The protection of personal and private information
- Affected – All Electronic Commerce conducted in Canada
- Enforcement and Penalties – Government intervention and publication of offenders

DATA PROTECTION ACT (UK)

- Intent - To safeguard the storage and handling of personal information
- Affected - All industries and business in the UK
- Enforcement and Penalties – Provides for criminal and civil fines



About J.Gold Associates

Founded by an internationally recognized expert and industry veteran with over 35 years of experience in engineering, product marketing, market research and analysis, and technology advisory services, J.Gold Associates provides its clients with insightful, meaningful and actionable analysis of trends and opportunities in the computer and technology industries. We offer a broad based knowledge of the technology landscape, and bring that expertise to bear in our work. J.Gold Associates provides strategic consulting, syndicated research and advisory services, and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies.



J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA
+1 508 393 5294
www.jgoldassociates.com