Gamma Solutions

**White**
Paper

# COMPLIANCE AND MOBILE COMPUTING

Intermec®
Honours Partner

Welcome to the age of regulatory compliance aimed at data integrity. Compliance has become one of the hottest buzzwords of the IT industry, and concerns for data protection and personal privacy warrant a growing body of legislation.

Although the number of regulations and the language in which they are written can be intimidating, all compliance legislation is written with two common goals: to protect networks from unauthorized access and to protect the data within that network.

Information Technology departments are charged with evaluating, updating and creating policies and procedures around every aspect of information security, so now is the time to become familiar with the regulations that apply to your specific business sector. New regulations include the UK Data Protection Act, EU Data Directive, Gramm Leach Bliley, Sarbanes Oxley, California SB1386 and PIPEDA (Personal Information Protection and Electronic Documents Act).

## What is Compliance?

Compliance is the act or process of meeting rules. It doesn't matter where those rules originate or what kind of rules they are. Simply meeting them means that you're in compliance. Here are brief summaries of the most widely enacted compliance regulations in use today.

**UK Data Protection Act – 1998**

This legislation states that data must be processed fairly and lawfully, must be accurate and kept up to date, kept no longer than necessary, kept secure and processed in accordance with individuals' rights. The details of this act are very complex, and may not be intelligible to those untrained in legal and IT jargons.

**EU Data Directive – 1995**

Specifies that any data stored (on a computer or even by pen and pencil) about any person – either directly or indirectly identifiable – is "personal data." Such data storage is only permitted for specified, explicit and legitimate purposes, in adequate ways, and must be kept up to date and in an identifiable format.

**PIPEDA – 2004**

The Personal Information Protection and Electronic Documents Act protects the use of personal information in Canadian commercial activities. PIPEDA was enacted to alleviate consumer concerns about privacy.

**Sarbanes-Oxley Act**

This United States law requires chief executives of publicly traded companies to personally validate the accuracy and reliability of financial statements and other information. The law was enacted to restore the public's confidence in corporate governance, as it ensures that internal controls govern the creation and documentation of information in financial statements.

**Gramm-Leach-Bliley Act**

The Gramm-Leach-Bliley Act applies to any company or organization that collects consumer financial data, and mandates that the data is protected via effective internal controls.

**California SB 1386**

California's SB 1386 requires entities or individuals doing business in California to notify state residents when unencrypted personal information is reasonably believed to have been compromised. There are no specific requirements for encrypting personal data, but information that is stolen in encrypted format is exempt from the data-owner notification requirement.

**Health Insurance Portability and Accountability Act (HIPAA)**
HIPAA is an initiative to develop standards and requirements for the secure transfer of any patient information including insurance, ID and health information that identifies individual patients. Non-European countries that have recently enacted data protection legislation applicable to the private sector include Hong Kong, New Zealand and Taiwan. To learn more about international privacy laws and commissions, visit the *International Access and Privacy Laws and Commissions (Department of Justice Canada)*. http://canada.justice.gc.ca/en/ps/atip/Internal.html

## IT Security and Compliance

IT systems generate, update, store and transport business-critical data, so corporations must ensure that the information is secure and can withstand audit scrutiny. To accomplish both these objectives, IT departments must establish infrastructures that secure data and applications while providing detailed reports for auditors.

The statutes listed above provide no specific guidance as to what must be done to secure data, but instead focus on the planning and processes required to ensure compliance. No regulation explicitly states that companies must use 128-bit encryption or specifies a schedule for updating antivirus signature files. The regulations instead outline the legal repercussions when data is exposed in an unauthorized manner. In many ways, regulatory compliance acts as an ad hoc security standard.
Regulations can be used as a security investment roadmap, but compliance does not necessarily equate a great security program. Companies must take care to look beyond the regulations and build a security program that not only meets regulatory standards, but suits the business as well. To that end, auditors and analysts agree that compliance efforts should focus on data encryption, user authentication and user-rights validation.

## Mobile Applications Bring New Risks

Mobile and wireless technologies require a revised strategy to achieve information security, as data is no longer contained within the four walls of the corporation. Sources such as Gartner and IDC estimate that more than half of global 2000 companies will make corporate applications accessible to the mobile user in 2005. Executive communications, e-mail, corporate directories, and calendars are just some of the sensitive organizational data stored on these devices.

Additionally, many companies, such as those with field service fleets, use mobile devices to store sensitive customer data, including credit card information. Gartner estimates that 90% of fleet devices have inadequate security. Too often, mobile devices are lost or stolen and the data stored onboard is readily accessible to whoever finds it. What's more, a savvy hacker can use the registry or passwords stored on a mobile computer to penetrate the enterprise.

Wireless technology is a far-reaching term that can signify wireless local area (WLAN or Wi-Fi); wireless wide area (WWAN), such as CDMA or GRPS; Radio Frequency Identification (RFID); or personal area networking technologies such as Bluetooth. With these technologies, data can be transmitted anytime, from any location. However, with the physical freedoms inherent to wireless technology come new security concerns. For more information on securing these technologies see **White Paper – Securing Wireless Technology.**

Achieving regulatory compliance while allowing mobile workers the freedom and productivity of secure wireless communication requires effort. However, expending these efforts brings an increased level of employee and customer trust in the company network and its health.

## AIDC Applications and Compliance

Automatic identification and data capture (AIDC) applications are common in industry, retail, consumer goods, logistics and government. These applications typically identify, track and manage asset and other inventory-related information. Mobile devices that employ barcode or RFID readers are used in these applications, communicating the collected data back to host computers either via Ethernet, WLAN or WWAN.

Inventory amounts, values and movement are tracked by Warehouse Management Systems (WMS), Work-In-Process (WIP), Retail Store Operations and Management applications, which process data that directly correlates back to the financial status of the company, its suppliers and/or customers – valuable information in need of protection.

Field Service, Direct Store Delivery and In-Transit visibility applications and the devices on which they reside often house consumer-account lists or even allow purchase transactions in which a consumer's credit card info is recorded.

All of these types of applications are addressed by one or more of the regulations previously discussed.

## Steps to Securing Mobile Applications

One of the best methodologies to ensure compliance is a layered security architecture, combined with best practices for administering, managing, and monitoring the layers. A layered security strategy should include the following action items.

1. **Assess the Risks**
   Considering the potential threats, vulnerabilities and operational risks posed to the network, the company should ask:
   - Is remote access a business necessity or just a convenience for employees?
   - Must employees access corporate network resources from home?
   - Do employees require access privileges to sensitive corporate information and applications?
2. **Conduct Annual Security Policy Audits**
   Companies are in a constant state of change. An annual security-policy audit can align the company's current need for compliance with the proper security measures.
3. **Require Authentication and User Credential Protection**
   - Ensure that all communications that travel from the corporate offices through the firewall are validated by digital certificates.
   - Protect user credentials, starting at the client device and extending all the way to the enterprise network.
   - Deploy advanced authentication and password encryption. Advanced authentication systems employ additional security measures such as tokens and digital certificates to validate a user's identity and initiate a unique network session.
   - Encrypt all stored data. This should include data stored on mobile-computer hard drives, SD cards, CF cards or other storage devices.
4. **Actively Manage Passwords**
   - Insist on passwords that are complex enough to withstand dictionary attacks, yet memorable enough that they will not be written down or forgotten.
   - Require minimum password lengths using alphanumeric characters.
   - Require password changes at regular intervals.
   - Assign separate credentials and passwords to each employee, rather than allowing multiple users to share credentials.
   - Disable any password auto-save features, as they can turn a stolen or compromised mobile device into an open door to the network.

5. **Ratchet Down The Firewalls**
   - Limit inbound traffic to one service provider's IP address.
   - Restrict Internet access from countries that your employees do not visit, reducing the risk of hacking or cyber-terrorism.
   - Close unnecessary ports. Chances are, not all of the firewall ports are used for remote access.
   - Protect all mobile devices with a personal firewall, ensuring that it is enabled and properly configured before the device is allowed network access.
   - Limit mobile device synchronizations. Synchronizing a PDA with a virus-infected home computer can pass viruses to the enterprise network, and then on to the corporate network.
6. **Use Secure VPN Tunnels**
   High-speed broadband connections allow mobile employees to access the company network from home, a hotel and from public venues. Unprotected, these "always-on" links serve as back door entry points to the corporate network. VPNs are imperative to performing safe remote and mobile business transactions.
7. **Manage Security Policies Centrally**
   Security management is a multilayered process, and the distributed nature of remote network access adds further complications. Centralized management solutions allow for configuration and enforcement of policies that are tailored to each user segment, and simplify policy administration for both remote network access and third-party security products.
8. **Strengthen Wireless LAN (Wi-Fi) Security**
   The conveniences and productivity afforded by wireless access pose some risk to corporate data, so consider employing the following tactics to bolster wireless security.
   - Change the default administrative password of your wireless router/access points.
   - Use 802.1x and WPA security protocols.
   - Keep wireless router/access-point firmware up to date.
   - Turn down the transmit power.
9. **Educate Users about Network Security**
   Launching a security awareness campaign can do wonders to enhance network security. Many users do not understand the need to protect the network and are not aware of its potential vulnerabilities. Once users realize how a breech can affect the company, most employees will take steps to ensure data security.
10. **Use Monitoring and Management Tools to Refine Security Policies**
    Each of the regulations specified earlier in this paper requires some form of auditing. Monitoring tools will not only help your company maintain compliance, but will also help the IT staff spot potential abuses, refine security policies and identify end users who could benefit from additional training.

## Device Best Practices

The manner in which devices are used directly affects the network's security strength. There are two classes of mobile devices within each organization: company-managed systems and non-managed systems. Company-managed systems should be used with the following safeguards in place.

- **Apply Standard Images** – A standard image is the default combination of software that IT staff load onto all employees' laptops or desk tops. This image usually contains a specific version of the operating system, a firewall and antivirus software that are company approved and can be managed and audited. The company's technology support group, the security office and users should select standard images.
- **Require Power-On Passwords** – This minimum-level protection can prevent data theft if a device falls into the wrong hands through either loss or theft.
- **Enable Data Encryption** – Sensitive files require encryption, but ideally, everything stored on a mobile device, including registry settings and configuration files, should be encrypted as well. Also encrypt data stored on SD cards, CF cards and any other storage medium.

- **Use a VPN** – Devices that access the corporate network from outside the walls – either via the Internet, Wi-Fi hotspots, or cellular technology – must use a VPN for access. Communications back to the corporate network must be kept private; therefore no split tunnels are allowed. Most personal firewalls can be configured to disallow split tunnels.
- **Require Unique Credentials** – Unique credentials, such as tokens or smart cards, are non-repeatable and can be used only one time to access the network.
- **Get Regular Checkups** – Information that is accepted into the network from a remote device – through Ethernet docking, wireless transmission or a VPN connection – can carry malicious viruses or worms. Devices must be verified as having the current operating system, patch levels, personal firewall and antivirus software before network access is allowed.

Non-Managed Systems include the personal PDAs, smartphones and mobile computers carried by visitors to the network. As these devices are not "owned" by the company, their image cannot be controlled, and their network access is random or a one-time event. Employ the following tactics to ensure regulatory compliance and security while allowing non-managed systems to access your network.

- Authenticate the "visitor" device to the network, preferably through a web browser and an SSL session, thus avoiding a direct network connection to the corporate infrastructure.
- Use a scan agent to check that the device is "clean" prior to allowing network access. Scan agents can be downloaded onto the visiting device through a web browser. Once the device has been scanned for viruses or worms, it can initiate a limited SSL session.
- Initiate cache cleanup on visiting devices. Cache cleanups remove any temporary files or downloads that have been added to the device during the session, ensuring that the session cannot be mimicked at a later time.

## Summary

The regulations listed above were designed to protect customers and the companies that serve them. Furthermore, compliance is required for doing business in today's litigious environment. The easiest route to compliance is by protecting your company's network and wireless devices through data encryption, user authentication and user-rights validation. Enacting best practices for wireless network, device and application security not only will ensure that your company complies with regulations, but will protect your network as well.

Gamma Solutions Pty Ltd
9 Compark Circuit, Mulgrave, Victoria 3170 Australia 61 3 8562 3000