



*Wave EMBASSY® software and self-encrypting drives make compliance with Massachusetts' new data protection laws easy and affordable.*

## Massachusetts' 201 CMR 17 Data Protection Regulation Mandates Encryption for Customer Data

### Is Your Business Safe?

A lost or stolen laptop carrying sensitive or confidential data is a threat to an organization's reputation and credibility — and may even expose it to legal liabilities with steep financial penalties. With data theft on the rise, protecting sensitive customer information is no longer optional.

Even with stronger regulations and corporate security guidelines, identity theft is now the fastest-growing crime in the country, according to the U.S. Department of Justice. The Identity Theft Resource Center recently reported a 47 percent increase in the number of data breaches in 2008 compared to the previous year. In light of this growing threat, Massachusetts' Office of Consumer Affairs and Business Regulations issued new rules governing how companies protect personal information for all Massachusetts residents with whom they do business.

The law (201 CMR 17) recognizes that the vast majority of breaches involve lost or stolen laptops and that data encryption is an effective means of neutralizing consumer risk should a laptop go missing. 201 CMR 17 details a number of preventative measures businesses must take, including encrypting data, utilizing authentication protocols and ensuring strict access control measures. Proactive organizations are now learning how this new law will impact the way they do business and how they can achieve compliance, thereby avoiding potential fines and criminal penalties.

### Smart Steps to Ensure Compliance

**Data Encryption:** 201 CMR 17 explicitly mandates encryption of all personal information stored on laptop computers.

**Automatic vs. Optional Encryption:** Since compliance is not optional, data encryption shouldn't be either. Relying on employees to know what to encrypt and how is not in line with industry best practices.

**Access Controls:** 201 CMR 17 specifies access control measures to restrict file access to those who need such information to perform their job duties.

**Remote Administration of Access Controls:** The laptop presents unique challenges for network administrators seeking to modify or revoke user-access privileges. Remote administration tools can be used to invoke policies upon network logon.

**Remote Data Destruction:** Once sensitive data are no longer needed, they should be destroyed to reduce security threats. Remote data destruction falls under 201 CMR 17 requirements for identifying reasonably foreseeable security risks and is a "green" method of retiring hard drives.

**Audit Logs/Event Monitoring:** 201 CMR 17 mandates reasonable monitoring of systems, for unauthorized use or access. Remote administration tools, including audit logs, make it possible for businesses to monitor their security and respond accordingly.

## Encryption Made Easy

*Factory-installed for greater protection and peace of mind*

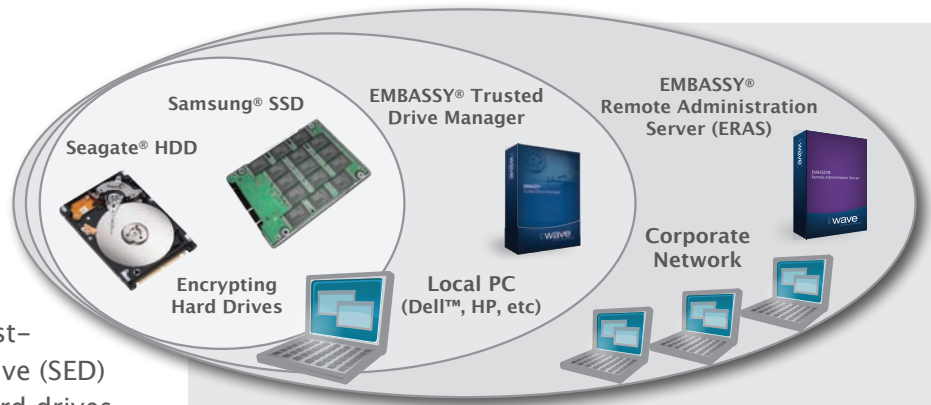
Wave Systems has partnered with leading drive manufacturers, Samsung Electronics and Seagate Technology, to offer the easiest-to-use and most secure self-encrypting drive (SED) solutions available. These industry-standard drives protect data where it lives — on the hard drive, by taking advantage of its closed environment to isolate data storage for stronger protection.

Wave's EMBASSY® Trusted Drive Manager is a client application that enables self-encrypting drive security features and allows for their local management. Preboot access control, password management and secure erase are just a few of the features provided.

Since self-encrypting drives and Wave Trusted Drive Manager ship factory-installed from leading PC vendors, businesses can easily add hardware-based encryption and authentication out of the box – saving time and money.

For a distributed network of self-encrypting drives, Wave's EMBASSY® Remote Administration Server (ERAS) provides robust policy management of users, credentials and access rights from one central location. Through native integration with existing directory structures and policy distribution mechanisms, assigning users and policies can be performed within the directory framework – dramatically simplifying deployment.

Given the increasing threat of security breaches and the fact that both individual companies and regulators are enacting strong data protection polices, encryption is no longer optional. While security best practices call for strong access controls and encryption, the bottom line also requires cost-effective solutions.



## Why Choose the Wave-Seagate Solution?

Out-of-the-box security greatly reduces total cost of ownership – simply set it and forget it

Hardware encryption is not vulnerable to traditional software attacks

Always-on industry standard AES encryption eliminates the IT learning curve

Remote drive management is essential for compliance reporting and significantly reduces ongoing management costs

Secure erase eliminates significant costs associated with wiping drives clean, providing a “green” alternative

HID iCLASS® contactless smart card and fingerprint authentication converge, simplifying enterprise access – reducing help desk calls associated with password reset

## Regional Sales Contacts

● **Kevin Baxter**  
Western Region  
925-462-1118  
kbaxter@wavesys.com

● **Don Hughes**  
Southwestern Region  
469-767-2025  
dhughes@wavesys.com

● **Jeff Walker**  
Midwestern Region  
763-478-5404  
jwalker@wavesys.com



● **Frances Rivoire**  
Great Lakes Region  
815-858-3437  
frivoire@wavesys.com

● **Patrick McCahill**  
Northeastern Region  
908-883-1041  
pmccahill@wavesys.com

● **Spencer Cobb**  
Southeastern Region  
678-705-3839  
scobb@wavesys.com

● **Martin Wargon**  
Federal and State Government  
561-752-4464  
mwargon@wavesys.com