

DeviceLock for SOX Compliance



Contents

- [Introduction](#)
- [SOX Requirements](#)
- [The Internal Control System](#)
- [DeviceLock from DeviceLock, Inc.](#)
- [How DeviceLock Supports SOX Compliance](#)
- [About DeviceLock, Inc.](#)
- [Contact Information](#)

Introduction

The Sarbanes-Oxley Act (SOX) was adopted in the US in 2002. This statutory act set out documentation and financial reporting requirements for companies, reinforced personal liability of CFOs and CEOs, and introduced procedures for regular independent audits.

Today, all public companies with stock listed on US stock exchanges are required to meet SOX requirements. Furthermore, a company's executive management - including the CEO and CFO - are held personally liable for ensuring compliance with the key provisions of SOX. Violations are met with hefty personal fines up to USD 25 million and prison terms of up to 20 years.

Despite its very stringent requirements, SOX has ultimately become the unspoken standard in corporate governance. Even companies that are not listed on US exchanges now prefer to incorporate provisions of this law in order to increase their competitiveness, attract more interest from investors and partners, and better protect their corporate assets.

The Sarbanes-Oxley Act does not pose direct requirements for corporate data security, although it does include a number of clauses concerning internal control, the completeness of sensitive financial documentation, and audit situations. Updating a corporate data security system can make compliance with the law's key provisions considerably easier.

This document will address SOX requirements that affect a company's data infrastructure, including the means of securing data collected and maintained by the company. It will also describe DeviceLock, a product from DeviceLock, Inc., which companies can use to more easily achieve strong compliance in the area of data security.

SOX Requirements

The Sarbanes-Oxley Act is comprised of sections, each of which sets out different corporate governance requirements. The key provisions of SOX are Sections 302, 404 and 802. These sections reinforce the personal liability of senior members of executive management, the need to maintain an internal control system, and the need to store all corporate correspondence.

Section 302. This section stipulates that CEOs and CFOs must include their own reports in audit records in order to authorize the accuracy of the information contained in the records. Managers who knowingly submit falsified reports or make intentional misstatements face serious criminal liability, including fines of up to USD 25 million and prison terms of up to 20 years.

Section 404. This section reinforces the need to implement an internal control system. An internal control system is necessary in order to promptly identify unauthorized or inappropriate use of company assets, including data assets. In other words, all operations - with digital company assets or financial reporting - must be meticulously controlled, and the company's infrastructure must include a fraud identification mechanism.

Section 802. In continuation of the previous section, this section stipulates that a company must ensure the storage of all business documents and any other kind of information relating to financial reports. Documents are to be stored for a minimum of 5 years. Additionally, Section 103 extends this to 7 years for any documents which may be involved in an audit. Note that SOX does not define exactly what data must be stored, and independent audit firms require the collection and archiving of an extensive range of electronic documents.

As a result, members of a company's executive management become personally and directly interested in ensuring compliance with SOX. Noncompliance can result in a legal investigation and criminal liability. Moreover, ensuring SOX compliance can also give a company a competitive edge and attract more investor interest.

The Internal Control System

The key requirements of SOX can be found in Section 404, which states that management must create an internal control system within the company. However, the law does not go into any detail about the system or what functions it must discharge.

These details are addressed in Auditing Standard No. 5,¹ a standard adopted by the Public Company Accounting Oversight Board (PCAOB) in 2007. The PCAOB oversees accuracy in reports issued by public companies and draws up standards which reinforce and elaborate on SOX requirements.

Auditing Standard No. 5 is to a large degree based on COSO's Internal Control - Integrated Framework standard.

Paragraph A5 in Appendix A of Auditing Standard No. 5 defines an internal control system over financial reporting as follows:

Internal control over financial reporting is a process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with GAAP and includes those policies and procedures that –

1. *Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;*
2. *Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and*
3. *Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.*

It is very important that the concept of "corporate assets" include the company's digital assets: intellectual property, commercial or technological secrets, and a complete spectrum of confidential documents. Clearly, the theft or leakage of this kind of data will impact a company's business, its financial indicators, and consequently, the company's shareholders. As a result, the

¹Auditing Standard No. 5: An Audit of Internal Control Over Financial Reporting.
http://pcaob.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf

internal control system must provide protection not only for financial reports themselves, but for the company's data assets as well.

DeviceLock from DeviceLock, Inc.

Opportunity for data leaks and theft is growing, particularly in light of the looming consumerization of corporate IT systems. The experts at Yankee Group and CSC Research confirm that IT department managers and directors cannot ignore the plethora of portable devices used by coworkers. They must provide support for employees' mobile computers. Otherwise, the company risks losing its innovative and competitive edge. Meanwhile, mass consumerism is rife with new and serious risks, since mobile devices may be used for fraudulent purposes, leaks, and internal breaches. DeviceLock can help solve that problem.

DeviceLock was designed for corporate users by DeviceLock, Inc. With DeviceLock, any size company can ensure maximum control over data which leaves the corporate network via workstation ports, wireless networks and external drives.

DeviceLock protects companies against leakage of digital assets and unwanted content, and serves as a tool for retrospective analysis of all data which company employees copy to external drives and take with them. DeviceLock also provides companies with the flexibility they need when working with mobile devices.

It is noteworthy that DeviceLock can be used to control a full range of potentially malicious devices: USB ports, disk drives, CD and DVD drives, FireWire, IR ports, parallel and serial ports, WiFi and Bluetooth adapters, tape recordings, PDAs, any internal and external removable drives and hard drives. DeviceLock conducts a thorough audit of user actions with these devices and data. Furthermore, DeviceLock includes protection against hardware keyloggers, which can be used to steal valuable data from coworkers' computers. Malicious users can connect this kind of device between an employee's computer and keyboard and trick antivirus software and other security software. When DeviceLock detects the exchange of data from the computer to the keylogger, it will warn the user and create a record in the events log.

What Does Gartner Say?

Companies should take 5 key steps in order to prevent the theft of intellectual property and confidential information:

1. Deploy content monitoring and filtering (CMF).
2. Encrypt backup copies.
- 3. Secure workstations, restrict home computers, and lock portable storage.**
4. Encrypt laptops.
5. Deploy database activity monitoring.

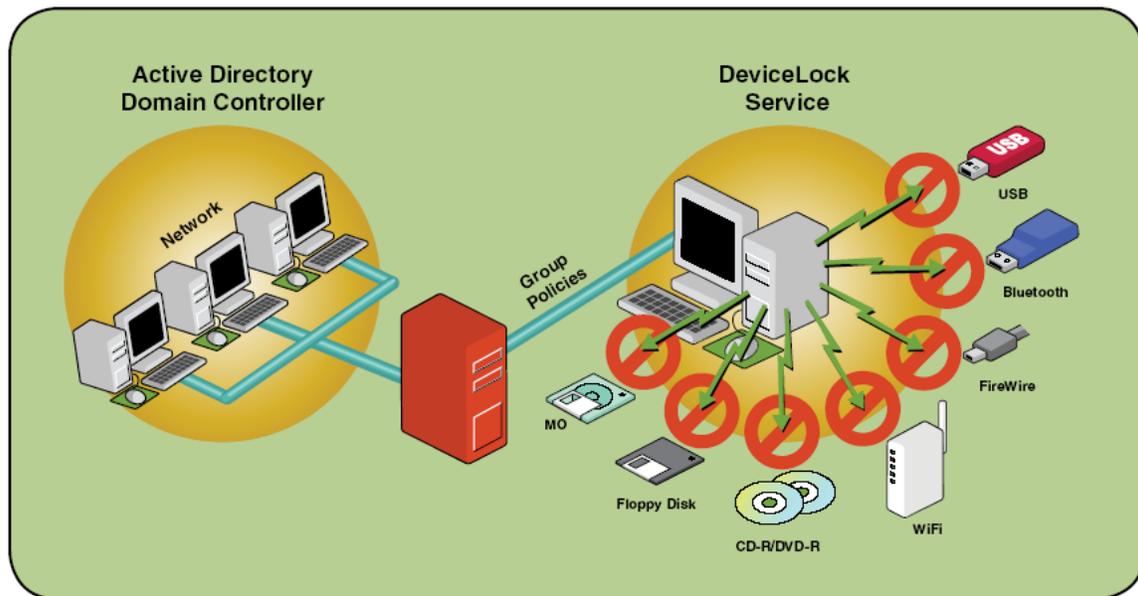
Source: [Gartner](#)

This product's main features include control over data exchange in line with defined policies and complete shadow copying of all outgoing data. While there are several solutions for storing email correspondence, only DeviceLock lets users gather and analyze data leaving the corporate network via workstation ports.

When the task at hand involves control over PDAs, smartphones and other devices, DeviceLock not only supports the shadow copying of all data transferred to a mobile device, it also allows flexible security policies and tracking the enforcement of these policies. For example, the product may allow a user to synchronize contacts and calendar, but prohibit copying files or synchronizing emails with attachments.

DeviceLock consists of three parts: the agent, the server and the management console:

1. DeviceLock Service (the agent) is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device protection on the client machine while remaining invisible to that computer's local users.
2. DeviceLock Enterprise Server (the server) is the optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock Enterprise Server uses MS SQL Server to store its data.
3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with three different management consoles: DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor).



DeviceLock can be controlled using group policies in Windows Active Directory, making it easy to integrate it into the infrastructure of an organization of any size.

How DeviceLock Supports SOX Compliance

DeviceLock controls data movement via workstation ports, wireless networks and removable drives based on flexible policies. Each time a request is made to move data to or from an external device, DeviceLock automatically decides whether to permit or prohibit access based on policies set by the IT security authority. DeviceLock settings and policies are easy to track, which is a SOX auditing requirement.

If fact, using DeviceLock in a corporate environment makes following the two main requirements of the law easier:

- **Section 404** stipulates that a company introduce and maintain an internal control system which covers financial reports and helps control the transfer of corporate assets. In this context, DeviceLock functions as a key element of the internal control system and helps manage access to a company's information assets at the workstation level and when dealing with mobile devices. Effective usage of DeviceLock will prevent leakage of intellectual

property and confidential documents, which could have major consequences for company shareholders.

- **Section 802** stipulates the archiving of all corporate correspondence which may be related to a company's financial reports, audits and standing. DeviceLock offers a one-of-a-kind feature: shadow copying of all or a necessary subset of data leaving the corporate network via workstation ports, removable drives, wireless networks and mobile devices. All data is stored in a database and accessible for subsequent audits and retrospective analyses.

The table below (Table 1) summarizes the features of DeviceLock and how they comply with SOX requirements.

Table 1. How DeviceLock can be used for SOX compliance	
SOX Requirements	DeviceLock Features
§802: archiving corporate information (primarily any outgoing electronic documents) with storage for a minimum of 7 years	Shadow copying of data which leaves the corporate site via workstation ports, external devices and drives, and wireless networks is one of DeviceLock's unique functions. The program saves all outgoing data on an external Microsoft SQL Server database, which helps when conducting subsequent audits, retrospective analyses and investigating instances of leaks, theft of data assets and other fraudulent acts.
§404: internal control mechanisms which hinder inappropriate use and theft of corporate assets	DeviceLock is an element of an internal control system, which ensures control over the transfer of sensitive documentation when it leaves a workstation via a port or wireless network. What's more, the product allows the use of flexible security policies when working with PDAs, smartphones and communicators, permitting some operations while prohibiting others. DeviceLock prevents leaks of confidential data and the theft of intellectual property and a company's data assets.
§302: personal liability of management for the accuracy of financial reports, the effectiveness of internal control and compliance with SOX	Thanks to DeviceLock, company management can remain calm and collected: according to the product's default policies, it prevents a company's information assets from theft. Moreover, the settings and policies are easy to audit. In addition to shadow copying, the product keeps an events log which reflects all of the actions taken by users to exchange data between a workstation and an external environment via ports and wireless networks. This kind of log is also a necessity when it comes to conducting successful audits of corporate data systems.

About DeviceLock, Inc.

DeviceLock, Inc. (formerly SmartLine Inc) was established in 1996 to provide effective and economical network management solutions to small, medium and large-scale business. Early on, we made it our mission to design software that is robust and reliable when it comes to enforcing network policy, while being easy and intuitive for system administrators to use. Furthermore, we made it our job to deliver solutions that are well-integrated and cost-effective. Based on this formula, we've introduced and developed category-leading products like DeviceLock for enforcing security policy related to personal devices.

DeviceLock, Inc. is a worldwide leader in endpoint device control security. Our DeviceLock product is currently installed on more than 3 million computers in more than 55 000 organizations around the world.

The company's customers include BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank, and various state and federal government agencies and departments.

DeviceLock, Inc. is an international organization with offices in San Ramon (California), London (UK), Ratingen (Germany), Moscow (Russia) and Milan (Italy).

Contact Information

DeviceLock Germany:

Halskestr. 21, 40880 Ratingen, Germany

TEL: +49 (2102) 89211-0

FAX: +49 (2102) 89211-29

DeviceLock Italy:

Via Falcone 7, 20123 Milan, Italy

TEL: +39-02-86391432

FAX: +39-02-86391407

DeviceLock UK:

The 401 Centre, 302 Regent Street, London, W1B 3HH, UK

TEL (toll-free): +44-(0)-800-047-0969

FAX: +44-(0)-207-691-7978

DeviceLock USA:

2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583, USA

TEL (toll-free): +1-866-668-5625

FAX: +1-646-349-2996

sales@devicelock.com

support@devicelock.com

www.devicelock.com