

## A Device Lock® Case Study: Washoe County, Nevada

### Abstract:

Washoe County, the second largest and most populated county in the State of Nevada, expanded its rollout of DeviceLock software to more than 3,000 endpoints across its network of government agencies as part of a security upgrade designed to ensure that the county's policies, procedures and security technologies are aligned with its data protection goals ahead of the January 1, 2010 effective date for Nevada's SB 227 data encryption law. DeviceLock enforces device-access policy that limits employees to connecting only Lexar JumpDrive SAFE S3000 encrypted drives to their office PCs and laptops.



**"DeviceLock has been our chosen endpoint DLP security solution for years, but its compatibility with Lexar JumpDrive SAFE S3000 USB flash drives at both the encryption detection layer and unique device ID number layer, along with its granular whitelisting features, really helps us with many levels of compliance as well as security,"**

**Christopher Long, CISSP  
Chief Security Officer  
Washoe County Technology Services**

**Identity Theft** is a growing issue around the world; however, the State of Nevada has had more than its share of cases in recent years. A 2006 Federal Trade Commission report estimated that for every 100,000 Nevadans, there were 130 cases of identity theft reported. To combat the problem, Nevada has been one of the most proactive states about introducing new legislation to enforce better data security among businesses that collect and store the personal identity information (PII) of its citizens. In March of 2009, Nevada Senate Bill No. 227 was signed into law which specifically requires the use of industry-standard encryption to protect any transmissions containing PII.

Longtime DeviceLock customer, Washoe County, Nevada, was well prepared for this new legislation. To be sure, when a government adopts laws designed to compel businesses in a specific direction, government agencies need to be ready for scrutiny vis-à-vis that legislation. However, compliance was achieved in a few straightforward steps. Washoe County expanded the rollout of DeviceLock software to more than 3,000 endpoints across its network of government agencies, and it upgraded any USB flash drives allowed to connect to the network to Lexar® JumpDrive® SAFE S3000 USB flash drives. These are validated for FIPS 140-2 Level 3 and offer AES 256-bit hardware encryption for protection of any sensitive information employees store and transport.

"Nevada is one of the states with the highest incidents of identity theft, ranking fourth according to a recent Federal Trade Commission report. Washoe County is modelling 'good security hygiene' designed to protect Nevadans from this trend," explains Ira Victor, principal of Data Clone Labs, the security system integrator under contract to Washoe County's IT department.

"Really, the law is catching up with the county, as Washoe has been proactive about setting up data protection policies and technolo-

gies for years, and is deploying the DeviceLock/Lexar media solution well ahead of any compliance deadlines. However, SB 227 does break new ground in that it defines these measures as a set of best practices for protecting personally identifiable information (PII) when it is being moved, both internally – for example, onto removable media like flash drives and CDs or smartphones, iPods or other user devices – as well as over the Internet. In addition, SB 227 offers the attractive incentive of 'safe harbor' from legal pursuit over purported PII leaks to any organization that follows the practices defined in the bill," observes Victor.

#### About DeviceLock

For organizations of any size and industry, DeviceLock software proactively protects endpoint computers against local data leaks and malware infiltration resulting from insider negligence, accidental mistakes or malicious actions. It enables IT security personnel to precisely control, log, shadow-copy and audit end-user access to all types of local ports and peripheral devices, including personal mobile devices, as well as local and network printers. Complementing its port, device, and data channel-based controls with data type-level security, DeviceLock supports true file type detection and filtering. In addition, DeviceLock blocks operations of USB and PS/2 hardware keyloggers.

#### About Lexar Media

Lexar Media is a leading designer, manufacturer, and marketer of NAND flash and DRAM memory products under the Lexar and Crucial® brand names. Lexar offers products in all major flash and DRAM memory categories, including consumer and enterprise-level USB flash drives, industry-leading memory cards for photography, and all popular form factors of memory cards for mobile devices. An industry leader in innovative, patented flash memory technology, Lexar is vertically integrated with Micron Technology, one of the largest semiconductor manufacturers worldwide. For more information about Lexar, visit [www.lexar.com](http://www.lexar.com).

### Key Points

- ▶ **Industry:** Government
- ▶ **Security Goals:** PII protection; Compliance with Nevada SB 227
- ▶ **DeviceLock Role:** Enforce use of only Washoe County-procured Lexar USB flash drives and other specifically approved USB devices.
- ▶ **DeviceLock Console:** MMC snap-in console for Active Directory Group Policy
- ▶ **Approved Encrypted Devices:** Lexar® JumpDrive® SAFE S3000 Series\*

"Washoe County

is modelling

'good security

hygiene' designed

to protect

Nevadans from

this trend,"

Ira Victor

Principal

Data Clone Labs

**DeviceLock**  
Proactive Endpoint Security

2440 Camino Ramon, Ste. 130

San Ramon, CA 94583, USA

email: [us.sales@devicelock.com](mailto:us.sales@devicelock.com)

Toll Free: +1 866 668 5625

Phone: +1 925 231 4400

Fax: +1 925 886 2629

The 401 Centre, 302 Regent Street

London, W1B 3HH, UK

Toll Free: +44 (0) 800 047 0969

Fax: +44 (0) 207 691 7978

Via Falcone 7

20123 Milan, Italy

Phone: +39 02 86391432

Fax: +39 02 86391407

Halskestr. 21

40880 Ratingen, Germany

Phone: +49 2102 89211-0

Fax: +49 2102 89211-29

© Copyright DeviceLock, Inc.

All Rights Reserved.

DeviceLock is a registered trademark.