

# America's Leading Universities Choose Druva inSync to Protect Critical Data on Laptops



“With inSync I can just walk in, administer backups based on the centralized administration and reporting system and walk out.”

**Dave Underwood, Principal IT Specialist**  
**Division of Agriculture and Natural Resources**  
**UC DAVIS**  
UNIVERSITY OF CALIFORNIA

## Why Universities Need Laptop Data Protection

With an intake of 20.4 million students, American Universities offer a wide range of educational programs to both domestic and international students through various campuses spread across the country. Thousands of students increasingly enroll for online programs as well. University staff members carry laptops that include course materials, research transcripts, student records including social security numbers, staff details, email interaction and medical and financial information, all generating terabytes of critical data.

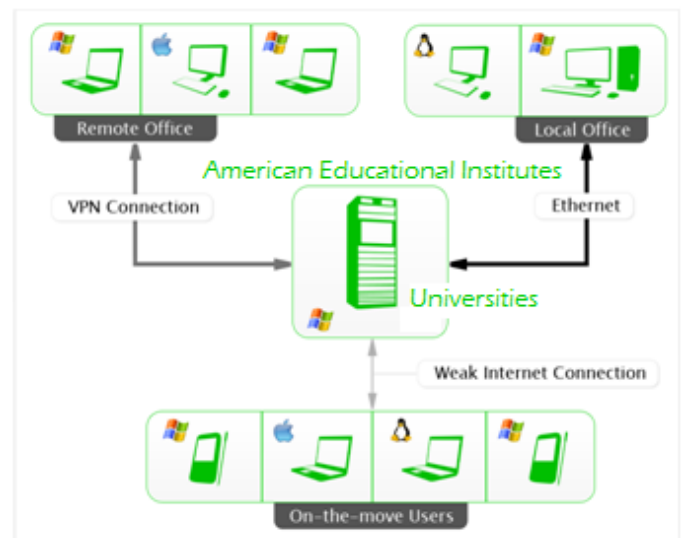
Given the sensitive nature of this data, universities need to protect it with the increased risk of lost or stolen laptops due to their portability. As a recent example, the University of California, Berkeley, had to deal with the theft of a laptop computer on campus containing the names, Social Security numbers and other personal information of 98,000 graduate students and applicants. To tackle such increasing instances of data loss, universities need a comprehensive data protection solution that begins with data backup and recovery.

## Business Case

### The Challenge

Universities encounter a number of challenges in their data protection attempts, including:

- ✓ Staff members do not equate lost laptops to loss of critical university data
- ✓ Critical research data is stored on laptops and only on laptops as primary work system
- ✓ Multiple platforms like Mac, tablets, etc., call for a **heterogeneous solution**
- ✓ Lack of uniform backup and security policies across multiple departments, campuses *and* mobile staff members
- ✓ Difficulty of deployment and administration of backup and restore policies
- ✓ Exploding storage growth across different campuses
- ✓ Continuous threat of unauthorized access
- ✓ Limited IT budget



The sheer volume of data and a need to maintain long-term records necessitate a secure and reliable backup solution that has low network overheads, is scalable enough to handle rapid data growth and capable of maintaining multiple versions of records, and uses little storage space.

With a diverse workforce spread across independent campuses and departments that have differing policies on backup, user adoption, policy management, and troubleshooting add to the data backup and management concerns. Some features that universities consider critical in their backup solution include:

- ✓ Centralized administration of backup and retention policies
- ✓ Deduplication to save storage
- ✓ Smart bandwidth usage, especially over WAN networks
- ✓ Secure backup and restore over WAN
- ✓ Scalability of solution for handling critical data growth

“The data our users collect is a valuable, sometimes irreplaceable, resource and needs to be adequately protected. As users cannot be relied upon to backup data themselves, a centrally manageable solution is required incase a laptop is lost or damaged.

**Rajiv Shah, Manager, Jhpiego (Kenya and Nairobi) - Affiliate of Johns Hopkins University (Baltimore).**



## Key Constraints Posed by Traditional Backup Solutions

Universities need a solution that can be implemented across departments and campuses without causing distress to administrators or end users. They find traditional backup solutions to be ineffective because:

- ✓ They have high end-user reliance for initiating backups
- ✓ Majority traditional backup solutions don't support multi-platform heterogeneous deployment
- ✓ Their backup performance over WAN is poor
- ✓ They require exponential backup storage to handle growing data
- ✓ They offer no easy data access or restore

“Users are notoriously lazy about backups. It helps to have a backup solution ensure that I can set up automated backup times and omit the risk of data loss and excessive user reliance.”

**Dave Underwood, Principal IT Specialist, Division of Agriculture and Natural Resources, University of California, Davis.**

**Create New Profile**

General | Schedule | Resources | Backup Details | Notification | Restore

Maximum bandwidth over LAN: 50 KBps

Maximum bandwidth over WAN: 20 KBps

TIP: Set to 0 KBps or 100% for unlimited bandwidth.

CPU priority: 8

Allow the user to change network/CPU settings:

Per user quota: 0 GB

TIP: Set to 0 for unlimited quota.

Keep all backups for: 7 days

Keep weekly backups for: 8 weeks

Keep monthly backups for: 12 months

TIP: Set all three to 0 to keep all backups.

Cancel Next

## The Solution: Druva inSync

With Druva inSync, the Department of Agriculture at University of California, Davis put in place an automated data backup solution. The simple interface helped easy adoption, while data deduplication technology reduced storage and bandwidth overheads, making backups both fast and invisible. Druva inSync allowed secure remote backups while saving bandwidth and storage without compromising administrative and policy controls.

“Druva inSync is easy to set up and manage with low overheads on bandwidth and system resources. The deduplication is great for saving storage.”

**Dave Underwood, Principal IT Specialist, Division of Agriculture and Natural Resources, University of California, Davis.**

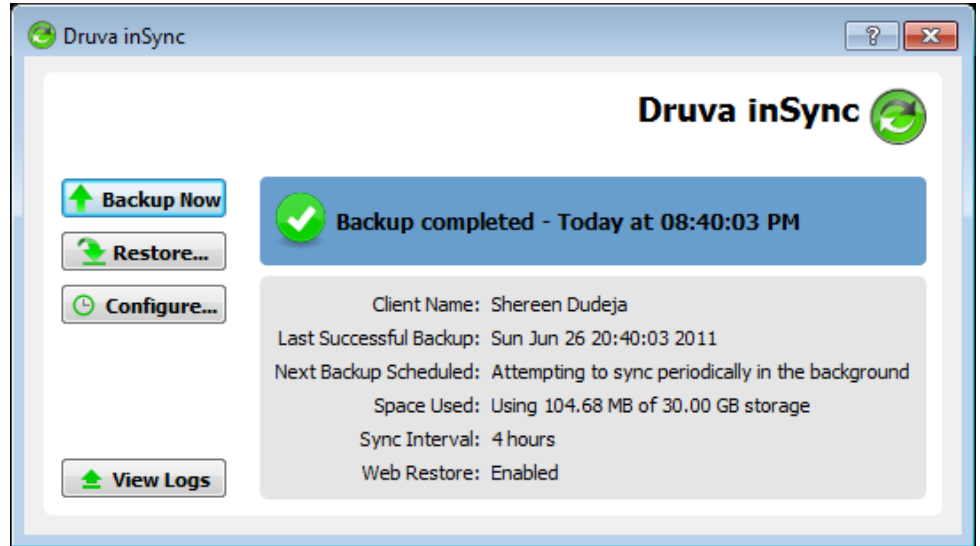
Druva inSync features patent-pending App-aware data Deduplication technology, which means faster backups and 90% bandwidth and storage savings. An innovative WAN Optimization Engine ensures that backups work efficiently on any network.

Druva inSync allows users to restore data on their iPad/iPhone and Android with a restore application designed specifically for these endpoint extensions. Users can securely view and access their previously backed up data from any point in time, enabling secure ready access to enterprise data.

Military-grade security of backups ensures that universities can fully address data security concerns while quick and multiple restore options empower users with ready-access to their data, wherever they are.

## The Results

- ✓ **Storage Savings:** By deploying inSync, several universities achieved **storage savings of up to 70%**.
- ✓ **WAN Optimized Backups:** Druva inSync considers the available network bandwidth and uses only a reserved percentage for backup as specified by the administrator. This feature allows remote users to backup their critical data despite having limited connectivity.
- ✓ **Military-Grade Security to prevent data loss and leakage:** Druva inSync features military-grade security, which makes backup and restore bulletproof. 256-bit SSL encryption ensures that the data is always secure on-wire. A 256-bit AES encryption standard at the storage layer prevents even the administrator from tampering data.
- ✓ **Centralized Administration for branch offices and mobile workforce:** Druva inSync has a powerful reporting engine and an interactive management console which allows the administrator to centrally view, track and schedule remote user backups at the most opportune times.
- ✓ **Simple Installation, Low Maintenance:** Druva inSync has a simple 20- minute setup and requires almost zero maintenance, freeing up IT administrators for more important or pressing tasks. Client updates are automatic and can be pushed out seamlessly, without impact to end-user productivity.



## Our Educational Institutes Customers Include:



## About Druva

Druva provides premium enterprise-class solutions for data protection and disaster recovery. Our products - powered by our patented App-aware Deduplication and WAN Optimization technologies - are changing the way enterprises manage and protect their endpoint data. For more information about Druva, please visit [www.druva.com](http://www.druva.com)