

## SOUTH FLORIDA EDUCATIONAL FEDERAL CREDIT UNION PROTECTS CUSTOMER DATA WITH DRIVELOCK



Credit unions are an important component of the financial system in the United States, Canada and many other countries. They perform many of the same functions as banks, but are member-owned and controlled. Like banks, they have a fiduciary duty to protect their clients' assets and confidential data, and this need is even more acute because the customers are also the owners. Implementing the technical means to protect data can be a challenge to many credit unions as they are often smaller organizations with a limited IT staff. This makes solutions that are easy to implement and easy to administer very attractive to credit unions.

### The Organization

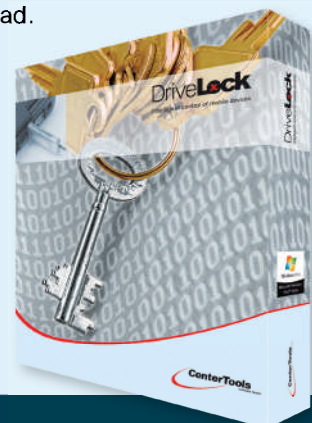
South Florida Educational Federal Credit Union (SFEFCU), was founded in 1935, by a small group of public school teachers and today serves the public school employees and students of Dade County, Florida and Miami-Dade Community College. It serves its members from four locations. SFEFCU offers a full range of banking solutions to its members. Its Web site is <http://www.sfecu.org>.

### The Challenge

Information technology plays a crucial role in SFEFCU's operations. Personal computers are an important part of all administrative functions and tellers also use PCs to record customer transactions. Access to financial data and other confidential information from these computers creates the risks of data theft and accidental data disclosure. SFEFCU's Board of Directors and Joe Lio, Director of IT Operations, have always been aware of this risk, but recent privacy legislation and new regulatory requirements have made the need to protect customer data even more acute. To address these requirements, the credit union has been implementing measures to protect data. The IT department realized that an effective security strategy must include measures to prevent that data is not copied from the credit union's computers without authorization. Initial investigations made it clear that existing tools could not provide the needed protection.

### Identifying a Solution

The IT department started by assessing risks to confidential data and identified the uncontrolled use of mobile storage devices and other peripherals as a key risk. An initial investigation into solutions ruled out entirely disabling USB ports because some critical business processes depend on the use of certain USB devices. Subsequently, several products were identified that could allow administrators to define which devices may be used. Most of these products were rejected because they couldn't provide enough granularity or because the infrastructure requirements were unacceptable. SFEFCU eventually chose DriveLock because it was the only product that provided the needed level of control and that could be implemented without purchasing additional hardware or adding a large administrative overhead.



Intelligent control of mobile devices made easy.

# DriveLock

Intelligent control of mobile devices

## Granular Control

SFEFCU uses DriveLock to ensure that only allowed peripherals are attached to its computers. For example, tellers must be able to use USB-connected check scanners but are prevented from attaching any other device to their computers. The use of memory sticks on most computers is restricted to IT staff. This prevents the unauthorized copying of data that could lead to the disclosure of confidential data and prevents the introduction of malicious software from removable media. DriveLock's integrated Device Scanner made it easy to identify all devices that were already in use and to create the rules required to allow their continued use.

## Implementation

After the testing phase was complete, the DriveLock deployment took only a few hours. DriveLock requires no servers to deploy and enforce its policies, so the main task was to configure Windows Group policy to mirror SFEFCU's IT guidelines for device usage. Once the policy was in place, the DriveLock Agent was rolled out to all PCs using a simple software deployment policy in Active Directory. Regular business operations continued throughout this process without any interruptions. Since the initial deployment virtually no ongoing administration has been required beyond occasional fine-tuning of the device usage policies.

## Results

With DriveLock, IT administrators can ensure that only approved peripherals are used and they don't need to

worry about data leaving the organization on removable storage devices. Detailed logging allows Joe Lio and his staff to confirm that the policies are enforced correctly, and continued periodic reviews of the logs alert them to attempts to bypass the security policy and to inadvertent actions that may endanger data security.

Users who have a business need to store files on removable media can continue to use approved storage devices without exposing the organization to the risk of viruses and other malicious software.

On the few occasions where Joe Lio has needed help with configuring DriveLock he has been very impressed with the quality and responsiveness of CenterTools' technical support.

## STATEMENT

**"After evaluating a few different products and solutions, DriveLock was by far the best one. There were a few that were similar in concept, but not as granular or as easy to configure. I would recommend this to any corporation that wants to control access to their systems via external media. Kudos to the developers."**

*Joe Lio, Director of IT Operations,  
South Florida Educational Federal Credit Union*

## CenterTools, LLC

1001 SW Fifth Avenue, Suite 1100  
Portland, OR 97204  
(503) 214-2887  
(888) 627-7515



info@centertools.com | www.drivelock.com

## SOUTH FLORIDA EDUCATIONAL FEDERAL CREDIT UNION PROTECTS CUSTOMER DATA WITH DRIVELOCK



Credit unions are an important component of the financial system in the United States, Canada and many other countries. They perform many of the same functions as banks, but are member-owned and controlled. Like banks, they have a fiduciary duty to protect their clients' assets and confidential data, and this need is even more acute because the customers are also the owners. Implementing the technical means to protect data can be a challenge to many credit unions as they are often smaller organizations with a limited IT staff. This makes solutions that are easy to implement and easy to administer very attractive to credit unions.

### The Organization

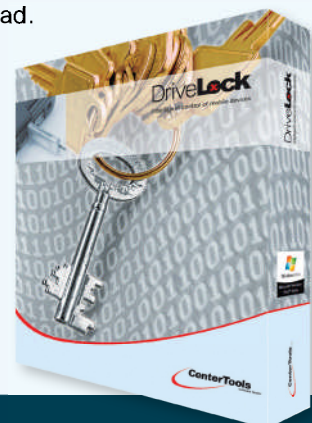
South Florida Educational Federal Credit Union (SFEFCU), was founded in 1935, by a small group of public school teachers and today serves the public school employees and students of Dade County, Florida and Miami-Dade Community College. It serves its members from four locations. SFEFCU offers a full range of banking solutions to its members. Its Web site is <http://www.sfefcu.org>.

### The Challenge

Information technology plays a crucial role in SFEFCU's operations. Personal computers are an important part of all administrative functions and tellers also use PCs to record customer transactions. Access to financial data and other confidential information from these computers creates the risks of data theft and accidental data disclosure. SFEFCU's Board of Directors and Joe Lio, Director of IT Operations, have always been aware of this risk, but recent privacy legislation and new regulatory requirements have made the need to protect customer data even more acute. To address these requirements, the credit union has been implementing measures to protect data. The IT department realized that an effective security strategy must include measures to prevent that data is not copied from the credit union's computers without authorization. Initial investigations made it clear that existing tools could not provide the needed protection.

### Identifying a Solution

The IT department started by assessing risks to confidential data and identified the uncontrolled use of mobile storage devices and other peripherals as a key risk. An initial investigation into solutions ruled out entirely disabling USB ports because some critical business processes depend on the use of certain USB devices. Subsequently, several products were identified that could allow administrators to define which devices may be used. Most of these products were rejected because they couldn't provide enough granularity or because the infrastructure requirements were unacceptable. SFEFCU eventually chose DriveLock because it was the only product that provided the needed level of control and that could be implemented without purchasing additional hardware or adding a large administrative overhead.



Intelligent control of mobile devices made easy.

# DriveLock

Intelligent control of mobile devices

## Granular Control

SFEFCU uses DriveLock to ensure that only allowed peripherals are attached to its computers. For example, tellers must be able to use USB-connected check scanners but are prevented from attaching any other device to their computers. The use of memory sticks on most computers is restricted to IT staff. This prevents the unauthorized copying of data that could lead to the disclosure of confidential data and prevents the introduction of malicious software from removable media. DriveLock's integrated Device Scanner made it easy to identify all devices that were already in use and to create the rules required to allow their continued use.

## Implementation

After the testing phase was complete, the DriveLock deployment took only a few hours. DriveLock requires no servers to deploy and enforce its policies, so the main task was to configure Windows Group policy to mirror SFEFCU's IT guidelines for device usage. Once the policy was in place, the DriveLock Agent was rolled out to all PCs using a simple software deployment policy in Active Directory. Regular business operations continued throughout this process without any interruptions. Since the initial deployment virtually no ongoing administration has been required beyond occasional fine-tuning of the device usage policies.

## Results

With DriveLock, IT administrators can ensure that only approved peripherals are used and they don't need to

worry about data leaving the organization on removable storage devices. Detailed logging allows Joe Lio and his staff to confirm that the policies are enforced correctly, and continued periodic reviews of the logs alert them to attempts to bypass the security policy and to inadvertent actions that may endanger data security.

Users who have a business need to store files on removable media can continue to use approved storage devices without exposing the organization to the risk of viruses and other malicious software.

On the few occasions where Joe Lio has needed help with configuring DriveLock he has been very impressed with the quality and responsiveness of CenterTools' technical support.

## STATEMENT

**"After evaluating a few different products and solutions, DriveLock was by far the best one. There were a few that were similar in concept, but not as granular or as easy to configure. I would recommend this to any corporation that wants to control access to their systems via external media. Kudos to the developers."**

*Joe Lio, Director of IT Operations,  
South Florida Educational Federal Credit Union*

## CenterTools, LLC

1001 SW Fifth Avenue, Suite 1100  
Portland, OR 97204  
(503) 214-2887  
(888) 627-7515



info@centertools.com | www.drivelock.com