CJIS ONLINE

Guide for Vendor Administrators

Contents

For more topics, please see our catalog of System User Guides on CJIS Portal.

CHANGE MANAGEMENT

Historical changes prior to 2017 can be requested from the CBI Crime Information Management Unit at cdps.cbi.ccic@state.co.us.

Version	Publish Date	Approved by
5.0	December 6, 2018	Emily C. Philip CJIS Information Security Officer/CCIC Supervisor
Summary of Changes		

- Added branding and formatting changes.
- Removed any outdated/inaccurate information.
- Updated Message Field Codes and Police Authority Levels for all forms.
- Added links to other chapters, policies, reference material, and outside resources as needed.
- Changed language from Vendor Services Coordinator to Vendor Administrator.

Version	Publish Date	Approved by
5.1	January 22, 2019	Emily C. Philip CJIS Information Security Officer/CCIC Supervisor
Summary of Changes		

- Revised instructions and screen shots to accommodate changes to CJIS Online.

Version	Publish Date	Approved by
5.2	December 5, 2019	Emily C. Philip CJIS Information Security Officer/CCIC Supervisor
Summary of Changes		

- Revised instructions and screen shots to accommodate login changes to CJIS online.

INTRODUCTION

The CJIS Security Policy states that "basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. […] Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained."

The CJIS Online utility is an optimal way to provide, certify, and track Security Awareness Training, and is required for vendors participating in the Colorado Bureau of Investigation's CJIS Vendor Management Program. This utility is offered free of charge.

After the organization's fingerprint/billing account is established, the CBI will create a Vendor Access account in CJIS Online and provide administrative access to the Vendor Administrator identified in the User Agreement and Account Application.

This guide is designed for the Vendor Administrator in order to assist with adding, modifying, tracking, and deactivating personnel.

Please contact the Colorado Bureau of Investigation at cdps.cbi.cjisvendors@state.co.us for any questions about this guide or the Vendor Management Program.

LOGGING IN

To log in as a Vendor Administrator, first visit www.cjisonline.com. Log in with your email address and the default password provided to you in your onboarding email. If you do not know your password, click **Forgot Your Password?** or contact the CBI.

The first time you log in, you will be asked to reset your password, and to review your information to make sure everything is correct.

DASHBOARD

The dashboard for all Vendor Administrators displays basic user statistics upon login.

These menu options are available at the top of the dashboard:

The Training menu allows the Vendor Administrator to access **their own training and testing** (if needed), as well as the ability to view their past certifications.

The Administration menu allows the Vendor Administrator to add, modify, and deactivate their own users, and to update their company information.

The Reports menu allows the Vendor Administrator report-building functions to see which users have taken tests or are soon expiring.
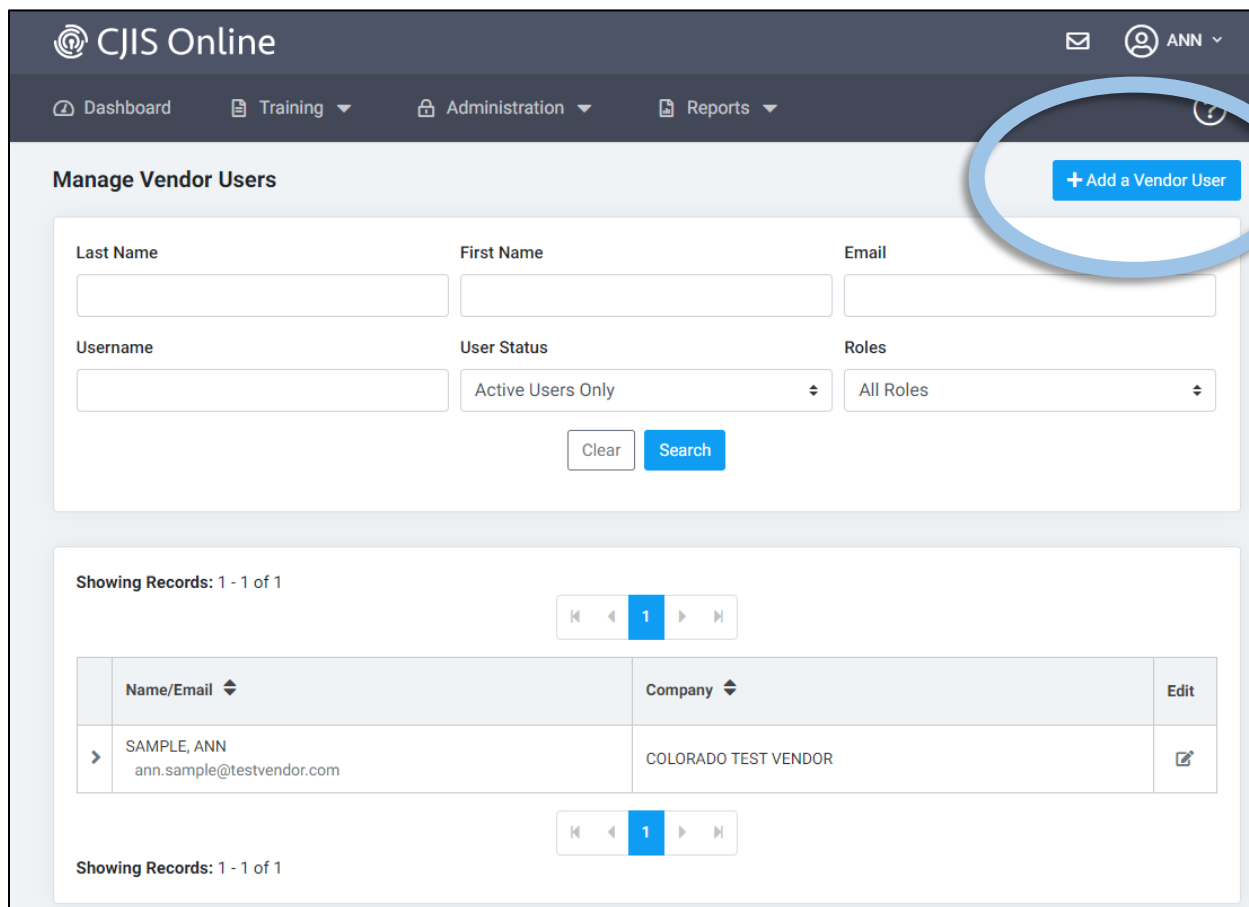
ADDING AND MANAGING USERS

To manage users, click on the **Administration** menu and select **Manage Vendor Users**.

By default, you will see a list of all employees listed under your vendor account.

You can search for employees added under your vendor account, and choose to filter by active and inactive. You can also add new users.

Adding a User

To add a user, click on the **Add a Vendor User** button.

Complete all personal details for the user as prompted.

A person's CJIS Online username will be their email address. This is preferred because they will receive email notifications regarding their certification status.

If they do not have an email address, tick the box for "This user does not have an Email Address", and create a username for them. We recommend a combination of the first and last name (e.g., terrysample or tsample).

When you are finished, click **Next**.

User Information

Select Company *

COLORADO TEST VENDOR

Choose a company or enter a name to search for a company

Last Name *	First Name *	Middle Name
Sample	Terry	

Phone	Phone Ext
303-555-9876	

Account Information

☐ This user does not have an Email Address

Email *	Confirm Email *
terry.sample@testvendor.com	terry.sample@testvendor.com

Username

When adding a user, Username is reserved for the user to set unless this user does not have an email

Password *	Confirm Password *
••••••••	••••••••

The password must be 8-20 characters long, must contain at least 1 letter and 1 number and not begin or end with a space.

Next →

Role Assignments

When creating a new user, it's important to select the correct Role Assignment.

In accordance with to the CJIS Security Policy, different levels of access to criminal justice information require different types of training.

Naturally, someone who has more of an information technology role at the organization would require more in-depth training than someone who may simply encounter a printout of a criminal history during the course of their duties.

Read the Level Assignment descriptions and determine which level applies to the employee.

Note: the Level 1 training and testing is available in both English and Spanish. The employee will choose which one they prefer when they log in.

Vendor Admins can elect to set up additional admins to assist them with managing employees; this is done by selecting the Vendor Admin Access button.

Credentials

Each user you add will log in with their username and a password that you create.

Please note, **when you add a new user to CJIS Online, it does NOT send an automatic notification to the user with their login information**. Vendor Admins will need to provide these new login credentials to employees.

A possible email template you can use is:

Dear [Employee Name],

The CJIS Security Policy written by the Federal Bureau of Investigation (FBI) requires that all individuals working for or within a criminal justice agency take routine Security Awareness Training if their duties put them in contact with Criminal Justice Information (CJI).

A CJIS Online account has been created for you to take the necessary training and testing required for your position.

Your credentials are as follows:

Username:

Password:

Please log into www.cjisonline.com to change your password immediately. You are required to take the necessary training within 6 months, and two years thereafter as long as you are in a position where Criminal Justice Information is being accessed.

Editing or Viewing Existing Users

To view or edit employee data, click on the **Administration** menu and select **Manage Vendor Users.** All users under your account will be displayed. You can use the search function to narrow down the display. Click **Edit** to view or modify employee information.

Editing a User

On the employee profile page, you have the option to edit their name, email address/username, and roles (click Save User when you are finished). You also have the ability to deactivate the employee (see below).

Viewing User Details

When an employee successfully completes their Security Awareness Test, their certification will display under the Certification Details tab. You can view their completion grade, as well as a copy of their certificate of completion.

Please note: there is a Fingerprinting section on this page. You may see data entered here from other states (if your company has customers there), but **Colorado does not use this function**. If you need to confirm whether fingerprints are complete for this employee, contact the CBI at cdps.cbi.cjisvendors@state.co.us.

Security Addendum Certification Signature Page

What Does This Mean?

If your company is what we call a CJIS Access Vendor[1], then **each one of your employees** with unescorted access to unencrypted CJI shall sign the Security Addendum Certification Page, per section 5.1.1.5 of CJIS policy. Your customers will request these signature pages from you, as will the CBI during an audit.

Effective 2019, CJIS Online provides a convenient way to upload and store these signature pages. If you choose to use this resource, follow these steps.

Note: if your company is a CJIS Support Vendor, this is not required.

Not sure what this document is? Please visit our CJIS Security Resources page, where you can find the Certification Signature page itself, as well as how it differs from the CJIS Security Addendum.

Uploading the Certification Signature Page

When you are in an employee profile (either immediately after you add them, or if you are editing an existing profile), you will see a Certification Details tab. The middle section of this page—labeled Documents—allows you to upload the Security Addendum Certification page.
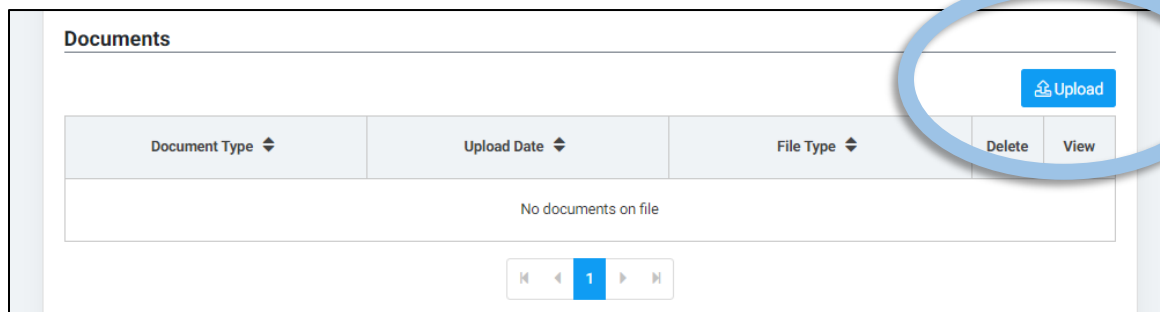
Choose the Document type (as of 2019, "Security Addendum Certification" is the only option).
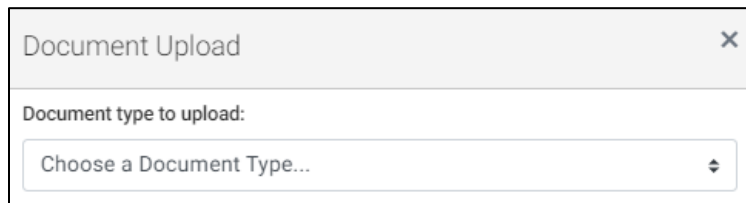
Browse for a file, or drag it directly onto the webpage (as of 2019, the upload function only accepts .PDF files). Then click **Upload**.

You will see the newly uploaded Certification page listed on the employee profile. From here, you can choose to view or delete the file.

---

[1] CJIS Access Vendors are vendors who support criminal justice agencies in a way that involves a higher level of access to CJI. In short, they access CJIS systems or media intentionally as part of their job function. This would include vendors that provide services such as IT support, software solutions that process or store CJI, drive sanitation/destruction, document shredding, encryption, cloud storage, etc.

Documents

Document Type ⇕	Upload Date ⇕	File Type ⇕	Delete	View
SECURITY ADDENDUM CERTIFICATION	December 05, 2019	PDF	🗑	👁

|◀ ◀ **1** ▶ ▶|

Removing Employees

If an employee no longer works for your organization, **deactivate them and notify the CBI immediately** at cdps.cbi.cjisvendors@state.co.us. To deactivate an employee, click on User Actions in their profile. Then select **Deactivate User** from the Dropdown Menu.

If they have been entered in error, contact cdps.cbi.cjisvendors@state.co.us to have them permanently removed instead of deactivated.

REPORTS

From the Vendor Admin dashboard, you will have access to different Reports options.

Test Activity Report

The Test Activity Report will display employees' test activity during a specified time frame.

User Status Report

User Status Report will provide a list of all employees and their Security Awareness Certification status.

Enter a date range, and select whether you want to see everyone who passed their test, everyone who failed, or both.

You can choose to export this list as a PDF file.

Expiration Report

The Expiration Report will display which users who are set to expire during a certain date range.

Employees will be notified by email 60 days in advance of when their certification is going to expire.

Please note, it is a condition of access to Criminal Justice Information Systems—and, in turn, participation in the Vendor Management Program—for these employees to keep their certificates active. When the CBI audits participating vendors, active and elapsed certifications are things we will review.