

Misuse & What NOT To Do

Regional Training 2023






mis·use

Verb

2/ use (something) in the wrong way or for the wrong purpose



Utah Code 53-10-108 (12) (a):

It is a **class B misdemeanor** for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by the division for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.



UCJIS USER SECURITY AGREEMENT

Per Utah Administrative Rule R722-900, a **USER** means a person working for or with an agency who has direct access to UCJIS or a **NON-ACCESS USER** who obtains UCJIS records from a person who has direct access.



UCJIS USER SECURITY STATEMENT

Dissemination, Privacy, and Security of Information: All of the information acquired from any file accessed in UCJIS, which includes Palantir, the Public Safety Alerts and Notifications System (PSANS), and NDex, is governed by regulations and policies of the FBI and the State of Utah. Dissemination, along with the privacy and security of any information acquired from any file in UCJIS, is for criminal justice purposes only. This information should be used for criminal justice purposes and criminal justice employment only. Printed copies must be destroyed by shredding or burning when no longer needed. Per the Administrative Office of the Courts, local agencies may NOT generate a hard copy of a juvenile's rap sheet or record summary.

User Security Agreement

Misuse of UCJIS information: Violation of dissemination, privacy, or security regulations may result in civil and/or criminal prosecution of the person(s) involved and loss of state computer access for the user and his/her agency. BCI maintains an automated dissemination log of all UCJIS file transactions to help ensure this information is being accessed for authorized purposes. Any unauthorized request or receipt of this information could be considered misuse. Utah Code Annotated 53-10-108(12) (a) states:

(12) (a) It is a class B misdemeanor for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by BCI or any information contained in a record created, maintained, or to which access is granted by BCI for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.

I, _____, have read and accepted the UCJIS User Security Statement and understand that I must abide by this agreement to have access to any information acquired through UCJIS.

Signature: _____ User ID: _____
Date: _____ Agency ORI: _____ Agency Name: _____

This agreement must be signed prior to accessing UCJIS or receiving any UCJIS information.
This form does not need to be signed for biennial re-certification.

Please submit this agreement to your BCI Field Services representative or bcifs@utah.gov per Utah Administrative Rule R722-900-4.

User Testing Agreement

UCJIS USER AND NON-ACCESS USER AGREEMENT

I certify that by signing this document that I have been trained and/or proficiency tested according to the procedure set by my agency, BCI, and CJIS. I accept that I will be held accountable for any information accessed under my user ID. I understand per Utah Code Annotated 53-10-108 (12)(a), it is a class B misdemeanor for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by BCI or any information contained in a record created, maintained, or to which access is granted by BCI for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.



UCJIS USER TRAINING AND TESTING AGREEMENT UCJIS NON-ACCESS USER TRAINING AGREEMENT



USER OR NON-ACCESS USER (Please Print)

USER OR NON-ACCESS USER ID

This agreement must be signed and submitted to BCI after the completion of the user or non-access user's initial training and testing *and* after each biennial training and testing.

UTAH ADMINISTRATIVE RULE R722-900 DEFINITIONS:

USER: a person working for or with an agency who has direct access to UCJIS.

NON-ACCESS USER: a person working for or with an agency who asks for and/or receives UCJIS records.

REQUIRED TRAINING OF EACH USER AND NON-ACCESS USER:

RESTRICTIONS ON ACCESS, USE, AND CONTENT OF UCJIS RECORDS: UTAH CODE 53-10-108
DISSEMINATION, PRIVACY, AND SECURITY OF UCJIS INFORMATION

ON:

ning

he procedure
d under my
person to
ich access is
nted by BCI

for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.

USER OR NON-ACCESS USER'S SIGNATURE

TAC SIGNATURE

DATE SIGNED BY TAC

AGENCY

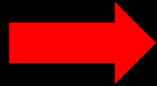
ORI

Please submit to your BCI Field Services representative or bcifs@utah.gov per Utah Administrative Rule R722-900-4

Revised May 2018



FBI



BCI



Criminal Justice
Agency

All Transactions In UCJIS Are Logged

BCI and the FBI can see :

- What was ran
- Who ran the transaction
- When the transaction was ran
- Why the transaction was accessed

CRIMINAL HISTORY QUERY

REQUESTER ORI	REQUESTER USER ID	REQUESTED FOR	PURPOSE CODE	AUDITING PURPOSE	FORMAT
UTBCI0000	cbakert	CBAKER	C	MISUSE PRESENTATION REGIONALS 23	



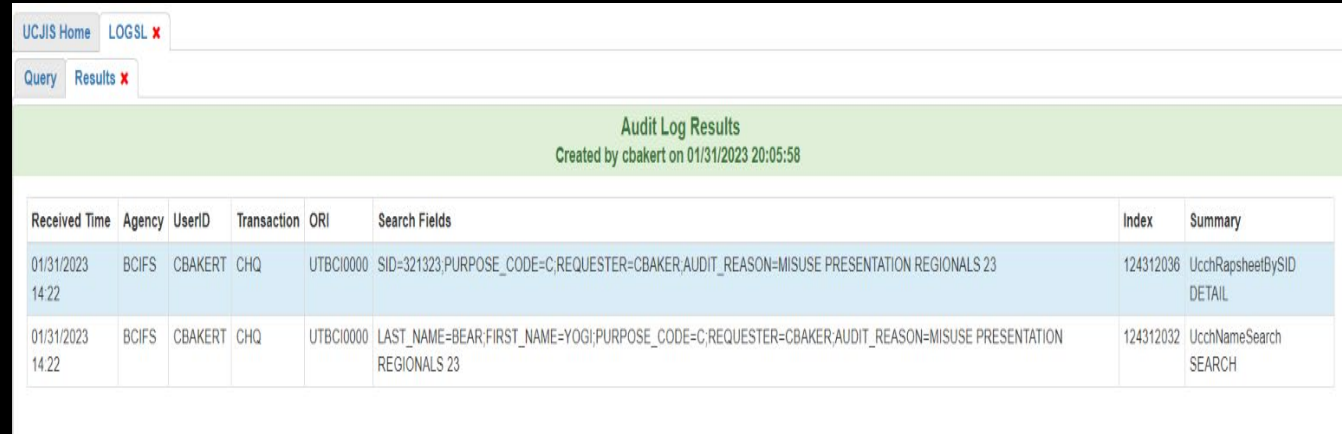
Dissemination Logs

LOGS Transaction: TAC's must periodically run the LOGS transaction to see what transactions users are running and to assist in the protection for your agency from misuse

Agency TAC's can view all transactions ran by users

Transaction LOGS

- Date / Time
- Agency ORI
- User ID
- Transaction
- Information Accessed



The screenshot shows a web application interface for UCJIS Home. At the top, there are tabs for 'UCJIS Home' and 'LOGSL x'. Below that, there are tabs for 'Query' and 'Results x'. The main content area is titled 'Audit Log Results' and includes a subtitle 'Created by cbakert on 01/31/2023 20:05:58'. Below this is a table with the following columns: Received Time, Agency, UserID, Transaction, ORI, Search Fields, Index, and Summary. The table contains two rows of data.

Received Time	Agency	UserID	Transaction	ORI	Search Fields	Index	Summary
01/31/2023 14:22	BCIFS	CBAKERT	CHQ	UTBCI0000	SID=321323;PURPOSE_CODE=C;REQUESTER=CBAKER;AUDIT_REASON=MISUSE PRESENTATION REGIONALS 23	124312036	UcchRapsheetBySID DETAIL
01/31/2023 14:22	BCIFS	CBAKERT	CHQ	UTBCI0000	LAST_NAME=BEAR;FIRST_NAME=YOGI;PURPOSE_CODE=C;REQUESTER=CBAKER;AUDIT_REASON=MISUSE PRESENTATION REGIONALS 23	124312032	UcchNameSearch SEARCH



Valid UCH Inquiry Purposes

- Detection
- Prosecution
- Rehabilitation of Offenders
- Apprehension
- Adjudication
- Correctional Supervision
- Detention
- Correctional Supervision
- Criminal Justice Employment
- Pretrial Release
- Post- Trial Release



Inquiring into any of the UCJIS files is NOT permitted for the following purposes:

- Curiosity and Personal Inquiries
- Employment for Non-criminal Justice Purposes
- Business Licenses
- Military Recruiters
- City/County Employees
- Citizen Advisory Boards, etc.

Scenario 1

The friend of the son of a deputy in your agency is pulled over. His background check reveals a history of violence, fraud, an NCIC known or suspected terrorist hit and several outstanding warrants. The deputy wants to know if anything came up on his check. Can he have this information?

Scenario 1 Answer

Dissemination of this information, even within the department, is not authorized in this situation. Unless there is a valid criminal justice purpose for the dissemination, what was found through UCJIS may not be passed to the deputy. If the information is passed, it is then considered to be a case of misuse.

Scenario 2

You have new renters for your basement apartment and want to screen them to ensure that you they don't have any outstanding warrants.

Scenario 2 Answer

This type of check is not authorized through UCJIS, however on the DPS public website, there is a link to check for warrants. If a UCJIS User completes this transaction it would be considered misuse.

- <https://bci.utah.gov/check-your-utah-warrants/>

Scenario 3

An officer took a screenshot from their RMS system, which was reflecting UCJIS information, and then posted it on social media as a public service announcement.

Is this considered misuse?

Scenario 3 Answer

This is considered unauthorized dissemination and therefore misuse. Although the individual may have had good intentions – it is still not allowed.

UCJIS information is protected and should not be shared with the public

Scenario 4

A city/county legislature or representative's aide wants to know who has parked in their parking spot or who has parked in the lot of the building. What information can you run and give to them?

Scenario 4 Answer

You cannot give them any information. They are not authorized to receive it. Even running this transaction is not for a criminal justice purpose and is considered misuse.

Scenario 5

If an officer is driving down the road and runs the license plate of the car driving in the other lane, to get contact information of the driver to ask them on a date, is this considered misuse?

Scenario 5 Answer

Yes, this is considered a curiosity check which falls under the qualifications of misuse.

Scenario 6

A user calls dispatch to run MMJL (Medical Marijuana transaction), is it considered misuse to disseminate their findings?

Scenario 6 Answer

The Dispatcher should verify the person is a Law Enforcement User, then they can run the transaction and disseminate according to their agency policy.

If the person is not Law Enforcement the transaction should not be completed. If it is, it then it would be considered misuse.

Some agencies/ users do not have permission to receive MMJL information.



Sharing CJIS Info With Another Agency?

Consider the following questions before disseminating:

- Do they have authorization?
- Why do they need this information?
- What is my agency's policy/procedure?

Internet Access to UCJIS

UCJIS is a web-based system that is being accessed from many different devices. This includes mobile devices such as smartphones, tablets, laptops, etc.

No matter which device is used, dissemination, privacy, and security laws governing misuse of UCJIS information all apply.



Laptop, Phone, & Tablet Access (MDM Policy)

Any portable device that is used to access UCJIS is under the same dissemination, privacy, security and misuse regulations as a desktop computer located in a locked office.





Working Remotely

Agencies should review their policies to see under which scenarios working from home is appropriate and which positions are authorized

Reporting security incidents for unauthorized access to CJI including unauthorized transfer of CJI to a non agency device should be included

Unauthorized individuals (family members, roommates, ect.) are not permitted to view CJI or operate devices that contain or can access CJIS



Creating A Controlled Area

Remote employees must designate areas where CJIS is stored or processes as a controlled area to properly protect CJIS

In a home environment, individuals must take necessary precautions to protect the information from not being disseminated to anyone who should not have it



At A Minimum

- Limit access to the controlled area
- Lock the area, room or storage when unattended
- Position devices to prevent unauthorized access/viewing of information
- Follow encryption requirements

Is it okay to print information from UCJIS?

Hard Copy Destruction

Cross-cut Shred



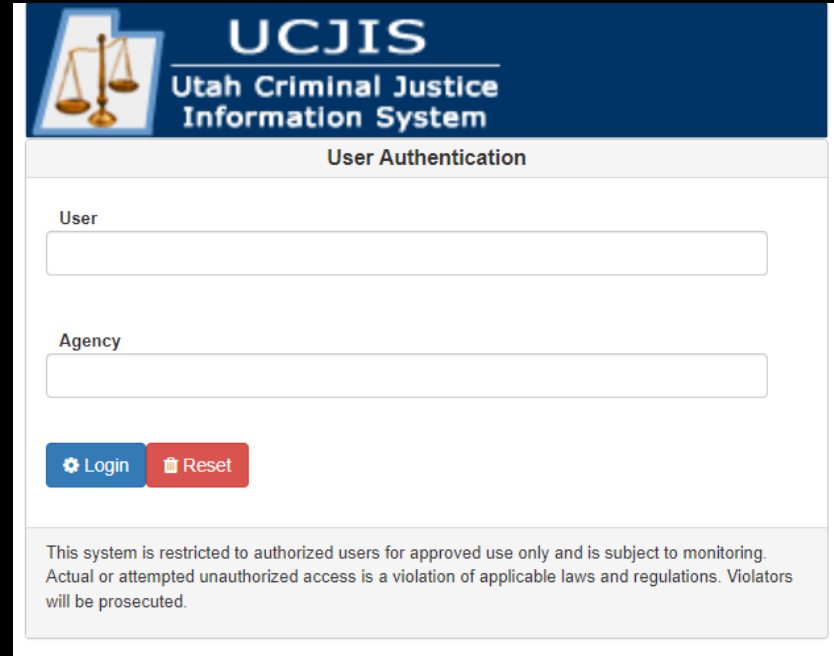
Or

Burn



UCJIS Test Account

<https://ucjis-test.ps.utah.gov/ucjis/#tree>



The image shows a screenshot of the UCJIS (Utah Criminal Justice Information System) User Authentication page. The page has a dark blue header with the UCJIS logo (scales of justice) and the text "UCJIS Utah Criminal Justice Information System". Below the header, the page is titled "User Authentication". There are two input fields: "User" and "Agency". Below the input fields are two buttons: "Login" (blue) and "Reset" (red). At the bottom of the page, there is a disclaimer: "This system is restricted to authorized users for approved use only and is subject to monitoring. Actual or attempted unauthorized access is a violation of applicable laws and regulations. Violators will be prosecuted."

UCJIS
Utah Criminal Justice
Information System

User Authentication

User

Agency

Login Reset

This system is restricted to authorized users for approved use only and is subject to monitoring. Actual or attempted unauthorized access is a violation of applicable laws and regulations. Violators will be prosecuted.

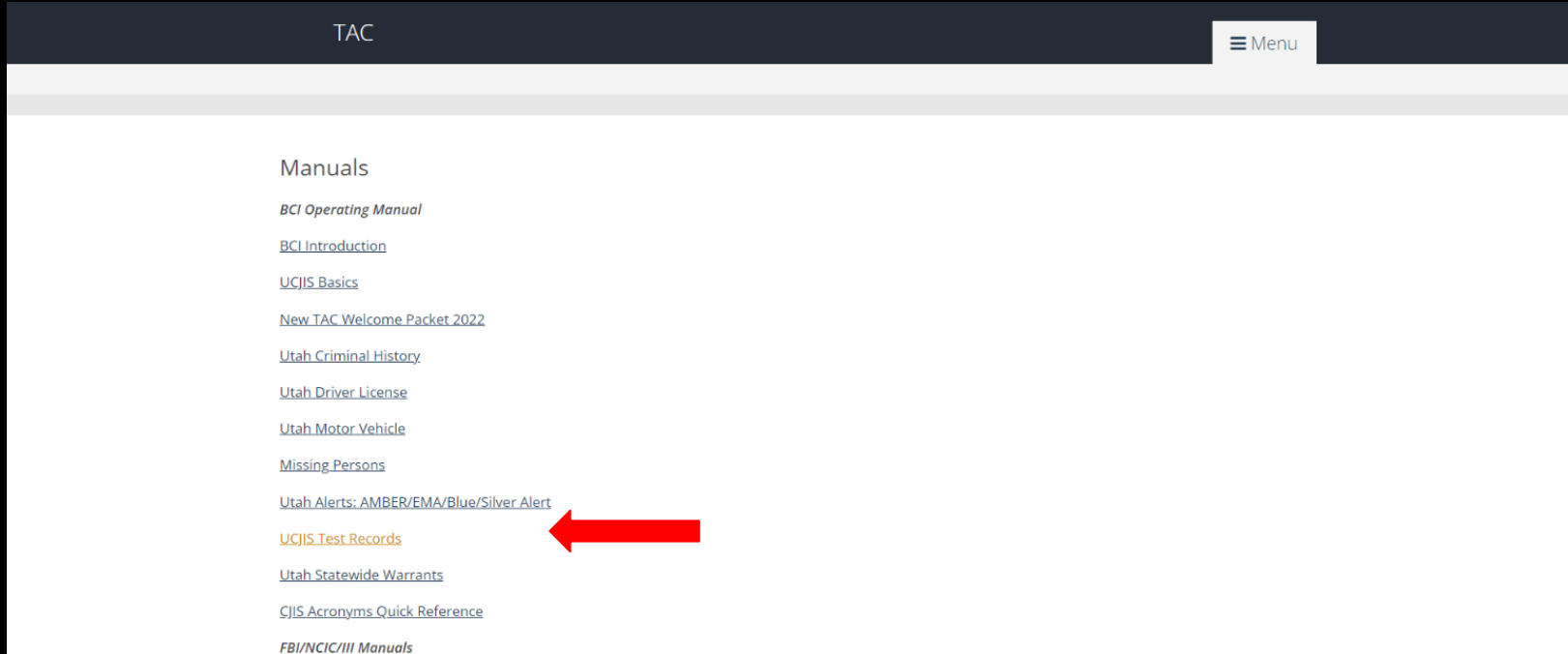


How To Setup A Test Account

Have your agency's TAC email your Field Service Representative

TAC it is not required but I have found it helpful if you have a test account created for yourself with the permissions your users will need to test it helps us to create your testing accounts quicker

Test Records To Use In Test Account



TAC

Menu

Manuals

- BCI Operating Manual*
- [BCI Introduction](#)
- [UCJIS Basics](#)
- [New TAC Welcome Packet 2022](#)
- [Utah Criminal History](#)
- [Utah Driver License](#)
- [Utah Motor Vehicle](#)
- [Missing Persons](#)
- [Utah Alerts: AMBER/EMA/Blue/Silver Alert](#)
- [UCJIS Test Records](#)
- [Utah Statewide Warrants](#)
- [CJIS Acronyms Quick Reference](#)
- FBI/NCIC/III Manuals*



Utah Motor Vehicle Test Records

Unlike most other files (Utah Criminal History, Utah Driver License, Utah Statewide Warrants, NCIC III, etc.) there are not always test records for Utah Motor Vehicle Transactions.

As of January 30, 2015, license AAA111 is a valid test record for MVQ. At any time, this record may be removed.

Remember, DO NOT use the license plate numbers of friends, neighbors, co-workers, etc., for use in testing or training. This is considered Misuse of UCJIS information.



What NOT To Do





NEWS

Officer allegedly used law enforcement system to get woman's name after he saw her shopping



By: [Brialey Dodson](#), [Mike Masciadrelli](#), [Nextstar Media Wire](#)
Posted: Dec 16, 2022 / 12:00 PM EST
Updated: Dec 16, 2022 / 02:25 PM EST

SHARE

OLD SAYBROOK, Conn. (WTNH) – A Connecticut police officer was released on bond Wednesday after allegedly accessing the Connecticut On-Line Law Enforcement Teleprocessing System to illegally obtain information on a woman he saw while on an assignment.

Josh Zarbo, a patrolman with the Old Saybrook police department since 2017, had looked up the woman's vehicle registration "for his own personal gain," according to police. He has been charged with third-degree computer crime, which is a felony.

Zarbo, 30, was on security detail at the Walmart in Old Saybrook on Black Friday to monitor activities inside and outside the store.

The arrest warrant states that when Zarbo saw the woman, he texted another officer to run her vehicle registration, and then asked for it over the radio system. After getting her information, he allegedly followed her on Instagram.



Josh Zarbo (Credit: Old Saybrook Police Department)

The woman told police that she saw Zarbo while shopping and later noticed that the man who followed her on Instagram was the same officer.

TRENDING STORIES

- 1 Burglars stole total of \$37K from Queens home: NYPD
- 2 Pregnant fiancée thrown from car in SI wreck: sources
- 3 2 men caught after 6 citywide

MANCHESTER, OH (FOX19) - A Manchester police officer accused of illegally accessing law enforcement databases has been indicted by an Adams County grand jury.

St. Louis County officer accused of illegally using police databases to look up information on 17 other officers

Charging documents said her department discovered she conducted 17 searches of fellow officers and one search of her mother between January and April 2020

LANESBOROUGH — It's not your personal Google. That's what Lanesborough Police Officer Brennan J. Polidoro was told after the town's chief determined that he violated state law by looking up women on a criminal justice database without a valid police purpose.



Actual Cases of Misuse

Officer purchasing firearm ran criminal history on previous firearm owner - disciplined by department

State employee exchanged criminal history record information for methamphetamines - criminal charges filed

Officer ran 'curiosity' record checks on women he met at a party - lost POST certification, terminated by department

State employee ran DL searches on coworkers to get Christmas card address list - disciplined by department



Recent Cases of Misuse

Multiple examples of users running themselves or coworkers when “testing” a transaction. Including scanning their own DL to test a patrol scanner.

Officer allowed teenage children to stay in office alone while responding to a call, which means they had unescorted access to UCJIS information.



Recent Cases of Misuse

UCJIS user that did not get along with their neighbor ran their criminal history and kept a file of it at their home. In a dispute, they not only had illegally run and printed the record but they shared it with other neighbors and their spouse.

UCJIS user ran their soon to be live-in girlfriend just to be sure about things before moving in together.



Reporting Misuse

For suspected misuse contact the following individuals to report:

The Director of BCI

Captain Greg Willmore

gwillmor@utah.gov

CC:

The Commissioner of Public Safety

Commissioner Jess Anderson

jessanderson@utah.gov



Questions?

