DAVE YOST
OHIO ATTORNEY GENERAL

BCI - Ohio Law Enforcement Gateway
Office (866) 406-4534
Fax (866) 750-0233

1560 St. Rt. 56, SW
P.O. Box 365
London, OH 43140
www.ohioattorneygeneral.gov

August 14, 2017

Dear Chief or Sheriff,

As a participant of OLLEISN (Ohio Local Law Enforcement Information Sharing Network), your agency had been sending a data extract file to OLLEISN from your RMS. Your continued participation is what makes OLLEISN an effective statewide investigative tool.

The Attorney General's office has been utilizing a Cisco 501PIX and SOHO Router as the methodology for your agency to send the extract file to OLLEISN. Due to the age of the PIX/SOHO technology, there are two new solutions for the sending and receiving of your extract file. Either option will eliminate the need for the Cisco PIX and SOHO.

The first option is to convert your OLLEISN submission method to version 2.2. This new version provides for the submission of additional data fields and only the data that changed since the last submission. For more information on how to update your RMS, log into https://www.ohleg.org. There you will find the "OLLEISN 2.2 Guide to Certification" and "OLLEISN 2.2 SDK" documentation.

For option 2, we are transitioning to a FTPS (File Transfer Protocol – Secure) method for the sending and receiving of your file. With the initiation of this FTPS solution, I am sending you information regarding the setup and use of FTPS. There is a user agreement form that will need to be completed and returned to the OHLEG Support HelpDesk, who will then have a username and password created for your agency. Please contact the OHLEG Support HelpDesk for the User Agreement. Once you have been notified of your account creation, you will then be able to do the extract file data transfer to OLLEISN.

If you have any questions regarding the form(s), or if you have questions regarding this process, please feel free to contact the OHLEG Support HelpDesk at 866-406-4534.

We look forward to working with your agency to effectively and securely receive your RMS extract file transfer and for the upload to OLLEISN.

Sincerely,

OHLEG Support

CP/lms
Enclosure

OHLEG
OHIO LAW ENFORCEMENT GATEWAY

FTPS – OLLEISN DATA TRANSFER

Set-Up Guide

This guide has been created to assist in setting up new law enforcement agencies with an FTPS (Secure File Transfer Protocol) account with the Ohio Attorney General's Office to allow them or their RMS vendor to transfer OLLEISN data securely via FTPS

**NOTE – This is for current certified agencies that are already transmitting OLLEISN data. For new agencies not certified please refer to http://www.olleisn.org/develop and the provider Implementation Guide.*

Requesting FTPS account for OLLEISN data transfer

1. The agency seeking an FTPS account, must have a FTPS (File Transfer Protocol) client to securely send OLLEISN data.
2. The agency must complete the most recent Ohio Attorney General Products and Services Standards of Conduct Policy User Acknowledgement form as shown in exhibit A.
3. The completed Products and Services Standards of Conduct Policy User Acknowledgement form will be attached to a new work order requesting the following:

   Please set up an FTPS account to transfer OLLEISN data for the following agency: ABC Agency ORI #OH123456.
4. The work order will go to AGO Security for review. Once security has approved and signed the agencies Products and Services Standards of Conduct Policy User Acknowledgement form the work order will go to systems to be set-up.
5. Once the FTPS account is set up, ITS support will contact the agency and provide them the user name, login and settings for the connection.
6. Should agency have any concerns with the connection they should contact ITS Support at 614-387-7644 and reference the work order number.

Exhibit A

DAVE YOST
OHIO ATTORNEY GENERAL

Information Technology Services
Office of the Chief Information Officer
Office 614-466-5272
Fax 614-644-2055

150 East Gay Street, 20th Floor
Columbus, Ohio 43215
www.OhioAttorneyGeneral.gov

Form ITSSEC01 Rev. 08-28-2018

Ohio Attorney General Products and Services Standards of Conduct Policy
User Acknowledgement

The purpose of this Acknowledgement is to ensure that any individual (the "User") accessing products and services of the Ohio Attorney General ("AGO") (including all AGO network services and data which may include, but is not limited to, FTPS, e-mail, source data, database services, and user account management ("Products and Services")) on AGO electronic networks become familiar with and acknowledge awareness of this Standards of Conduct Policy (the "Policy") when connecting to the AGO network from any host to utilize AGO Products and Services. This Policy is designed to minimize the AGO and the State of Ohio's potential exposure to damages which may result from unauthorized use of AGO Products and Services. Such damages include, but are not limited to, the loss or dissemination of sensitive or confidential data, loss or dissemination of intellectual property, damage to public image, and damage to critical AGO internal systems. Any violation of this Policy may result in immediate termination of User access to any or all AGO Products and Services and notification of the violation to the User's employer signing this Policy in conjunction with the User. **All Users will be held personally responsible and liable, to the fullest extent of the law, for actions in violation of this Policy.**

This Standards of Conduct Policy must be followed at all times. Therefore, all Employers and Users shall:

- Utilize AGO's network resources, applications, systems and any information provided therefrom for authorized use only.
- Take reasonable precautions to ensure that the computer used to connect to AGO Products and Services is secure and free of malicious code. Examples of reasonable precautions include, but are not limited to:
    - Endpoint protection (e.g. anti-malware, user controls, etc.),
    - Perimeter protection (e.g. firewall, Host/Network Intrusion Detection System, Host/Network Intrusion Protection System, Demilitarized Zone, Universal Threat Management, etc.),
    - Audit logs,
    - Adequate physical security for data and systems,
    - System monitoring and auditing of the logs,
    - Incident response policy, and
    - Data safeguarding procedures appropriate for the type of data and access.
- Protect against improper access, use, loss alteration or destruction of any AGO data. Examples of this protection include, but are not limited to:
    - Never sharing an account,
    - Reporting if the User has more access than needed,
    - Lock or log out of workstations when not actively using them,
    - Ensure workspaces are set up to prevent passersby from viewing any information,
    - Only using data or access to the data for the express authorized purpose,
    - Preventing the introduction of malicious code,

- Ensuring data is backed up or replicated, and
- Ensuring data is not copied or does not leave the work environment.

- Promptly notify the AGO if a Security Event has occurred or if suspicion of a Security Event has been identified. A Security Event includes, but is not limited to:
  - Any abnormality in the environment that could lead to a compromise of the system integrity or result in disclosure of data,
  - Hack attempts,
  - Malware,
  - Changes in security infrastructure,
  - System failures,
  - Compromised user accounts, and
  - Lost/stolen laptop or media.
- Promptly notify the AGO of the date of separation if User leaves the employer or if access to AGO networks, applications, systems and/or AGO data is no longer required. Access to AGO Products and Services may be rescinded for failure to provide such notice.
- Create a password in compliance with the AGO password criteria set forth below. The AGO reserves the right to change the password criteria from time to time. Compliance with the AGO password criteria will be enforced via automated password authentication or public/private keys with strong pass-phrases. The AGO password criteria are as follows:
  - Minimum 12 characters,
  - Must include 3 of the 4: a-z, A-Z, 0-9, and special characters,
  - Passwords will require being reset based on level of access at the AGO's discretion,
  - Passwords must be kept securely by the account owner, and never be shared,
  - Passwords must not contain sequences 01, 123, abc, etc.,
  - Passwords must not contain properly spelled dictionary words, and
  - Passwords must not be directly identifiable to the user (e.g. social security number, date of birth, spouse's name, username, etc.).

  Password history will be retained for 24 changes to ensure unique passwords. Inactive accounts will be disabled at 90 days, and removed at 120 days. Users of accounts that reach 120 days of inactivity must reapply for an account.
- Comply with all federal, Ohio and any other applicable law, including, but not limited to: Internal Revenue Service Publication 1075 which is based on United States Code Title 26, Section 6103; Ohio Revised Code Chapter 1347; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the associated omnibus rule to modify the HIPAA Privacy, Security and Enforcement Rules; and the Health information Technology for Economic and Clinical Health ("HITECH") Act.
- Comply with all applicable contracts and licenses.

USER'S UNDERSTANDINGS:

- User understands that any Users who engage in electronic communications with people or entities in other states or countries, or on other systems or networks, are on notice that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for obtaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
- User understands that the AGO retains the right, and has the capability, among other security measures, to review, audit or monitor the User's directories, files, e-mails (both sent and received), as well as Internet usage to ensure maintenance of system integrity. User also understands that User's access to the Products and Services is subject to termination for breach of this Policy at any point.
- User understands that, among other security measures, the AGO makes backup copies and stores User information. User activities are therefore not private and User content is potentially stored on AGO servers. User also understands that the AGO is subject to public records disclosure and to discovery requests and that User's activities and information may be released pursuant to a public records or discovery request.

PROHIBITED ACTIVITIES:

- Users shall not engage in illegal, fraudulent, or malicious conduct on or while accessing any AGO Product or Service.
- Users shall not provide an AGO Product or Service login or password to any person or entity for any reason.
- Users shall not leave a computer unattended that is connected to AGO Products or Services for any period of time unless it is secured in such a way that the computer cannot be accessed by any other individual (e.g. sign-off procedure, password protected screen saver, etc.).
- Users shall not engage in conduct on or while accessing any AGO Product or Service that is beyond the scope of the User's AGO authorized access, including access governed by a Memorandum of Understanding, contract or retention agreement, if applicable, for which AGO access is granted.
- Users shall not monitor or intercept the files or electronic communications of AGO employees or any other third parties.
- Users shall not attempt to test, circumvent, or defeat the security systems of the AGO or any other organization, or access or attempt to access the AGO's or any other organizations' systems without prior authorization from the AGO.
- Users shall not provide anyone access to AGO Products and Services.
- Users shall not provide anyone access to or disseminate any AGO information, regardless of whether or not it is considered confidential or public, and regardless of how the information was obtained, without prior authorization from the AGO.
- Users shall not make paper, electronic, or any other copies of any AGO information, regardless of how the information was obtained, without prior authorization from the AGO.

User Acknowledgement

By signing below, you, as a User, acknowledge that you have read and understand this Policy, and you, the User, agree to comply with the terms of this Policy.

Printed Name of User: _____ Title: _____

User's Employer: _____ Contract End Date: _____

User's Phone Number: _____ User's E-mail: _____

Requested Period of Access:
From: _____ To:_____

Application or resources requested:

(FTPS, Edisp, Livescan, etc.): _____

_____

Public IP: _____

User's Signature: _____ Date: _____

Account Identity Control Information (1): _____ (mother's maiden name, etc.)

Account Identity Control Information (2): _____ (first car owned, etc.)

The above Account Identity Control Information will be used to identify you in the event that you have lost or do not remember your account ID or password. The User must provide two unique pieces of information as a shared secret with the AGO to verify your identity when account resets and other services that require identity verification are needed. It is the User's obligation to provide and secure these shared secrets in the same manner that is required for account credentials.

Employer Acknowledgement

By signing below, you, as the User's employer, acknowledge that you are a duly authorized representative of the User's employer able to bind the employer to the terms of this Acknowledgement. By signing below, you, as the User's employer, also agree that access by the employer may be rescinded at the discretion of the AGO, with prior notice, if the employer fails to take reasonable precautions, as defined above, to avoid a breach of this Policy and/or to ensure that the employer's Users do not breach this Policy.

Printed Name: _____ Title: _____

Employer's Signature: _____ Date: _____

Employer's Phone Number: _____

Employer's E-mail: _____

Official AGO Use Only:

AGO ITS Work Order Number: _____

AGO issued username: _____

AGO issued rights: _____

_____

AGO Chief Information Officer, Chief Information Security Officer, or their designee

Printed Name:_____ Title: _____

Signature: _____ Date: _____

Comments: _____

_____

_____

_____

_____

_____

_____