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 ITSSEC02 Rev. 01-15-2019

Ohio Attorney General Non-Employee Computer Usage, Network Access, Internet Usage, and Social Media Policy
Contractor Employee Acknowledgement

This Ohio Attorney General ("AGO") Non-Employee Computer Usage, Network Access, Internet Usage, and Social Media Policy Contractor Employee Acknowledgement (the "Acknowledgement") sets forth the policies and procedures for proper computer, network, Internet, and social media use by all non-AGO personnel performing work for the AGO (the "User"). This Computer Usage, Network Access, Internet Usage, and Social Media Policy (the "Policy") applies to all independent contractors and/or any other consultant performing work for any contractor or consultant doing business with the AGO and their employees. Any violation of this Policy may result in, among other penalties and liabilities, immediate removal of User access to all AGO systems and notification to the User's employer of the violation. The AGO may temporarily suspend or block a User's access to an account when it appears reasonably necessary to do so to protect the security of the AGO network or to protect the AGO from liability. **All Users will be held personally responsible and liable, to the fullest extent of the law, for actions in violation of this Policy.**

I. COMPUTER USAGE AND NETWORK ACCESS POLICY

In order to comply with Ohio law and to ensure the security and integrity of AGO network resources (e.g. routers, switches, servers, workstations, printers, etc.), the User shall:

- Acknowledge he/she has been provided with and will comply with the provisions of this Policy;
- Utilize the AGO's network resources and any information/data provided therefrom for authorized use only;
- Use all computer resources, including, but not limited to, equipment, hardware, software, documentation, and data solely for AGO business;
- Immediately notify the AGO of any proven or suspected unauthorized disclosure or exposure of any AGO data or of information or identity theft;
- Immediately 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 the AGO network may be rescinded for failure to provide such notice;
- Take all reasonable precautions to prevent the dissemination of User's credentials by any means, including, but not limited to, not sharing the User's username and password, not writing down the username and password, etc.;
- 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 applicable network or operating system restrictions, whether or not they are built into the operating system or network, and whether or not they can be circumvented by technical means;
- 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; and
- Comply with all applicable contracts and licenses.

User shall not:

- Move, alter, delete, copy, or otherwise change any information/data stored or contained on AGO networks or computers without express, written authorization by the AGO (e.g. a written agreement, scope of work, or approved vendor quotation).
- Leave a computer unattended for any period of time unless it is secured in such a way that the computer cannot be used by any other individual (e.g. sign-off procedure, password protected screen saver, etc.);
- Make paper, electronic, or any other copies or reproductions of any AGO information/data or licensed materials, regardless of how the information/data or materials were obtained, without prior authorization from the AGO;
- Use an e-mail account, username, or signature line other than the User's own;

- Attempt to represent himself or herself as any individual other than him/herself. This specifically includes, but is not limited to, use of the Internet, e-mail, online service account, or signature line; and
- Share any information/data gained through use of AGO networks with anyone outside the AGO without prior authorization from the AGO.

II. INTERNET USAGE POLICY

Improper use of the AGO's Internet and Internet services can waste time and resources, violate AGO policies, and create legal liability and embarrassment for both the AGO and the User. The AGO's Internet services include, but are not limited to, e-mail, file transfer protocol, and access to the World Wide Web. This Policy applies to use of the AGO's Internet and Internet services (collectively the "Internet") accessed using AGO network resources or paid Internet access methods, and used in a manner that identifies the User with the AGO.

User's authorized Internet access will be provided by the AGO through vendors approved by the Information Technology Services Section of the AGO ("ITS"). All other access methods to the Internet are prohibited.

All activities that require use of the AGO's Internet must be pre-approved by the AGO. Certain activities that require use of the AGO's Internet are strictly prohibited. Therefore, the User shall not use the AGO's Internet in connection with any of the following activities:

- Engaging in illegal, fraudulent, or malicious conduct;
- Engaging in conduct that is beyond the scope of the contract or retention agreement, if applicable, for which User access is granted;
- Transmitting, downloading, retrieving, or storing offensive, obscene, defamatory, or otherwise prohibited material (including, but not limited to, pornographic, X-rated, religious, political, threatening, or racial or sexual harassing content);
- Harassment of any kind;
- Monitoring or intercepting the files or electronic communications of AGO employees or third parties;
- Attempting to test, circumvent, or defeat the security systems of the AGO or any other organization, or accessing or attempting to access the AGO's or any other organizations' systems without prior authorization from the AGO;
- Providing access to anyone other than the User to the AGO Internet and/or network resources without prior authorization from the AGO;
- Providing anyone access to or disseminating any AGO information/data, regardless of whether or not it is considered confidential or public, and regardless of how the information/data was obtained;
- Using or accessing social media;
- Participating in chat rooms, open forum discussions, interactive or instant messaging unless such participation is for business purposes and pre-approved by ITS;
- Operating a business for personal gain, sending chain letters, or soliciting money in any way for religious, political, charitable, personal, or business purposes while acting within the scope of User's work and using AGO Internet services;
- Transmitting, collecting, and/or receiving incendiary statements which might incite violence or describe or promote the use of weapons or devices associated with terrorist activities;

- Distributing frivolous, non-business related material such as jokes and or cartoons; and
- Participating in any other unauthorized activity that may bring damage, discredit upon, or create liability to the AGO.

III. SOCIAL MEDIA POLICY

Social media and social networking sites are not private and the User shall use good professional judgment regarding any references to the AGO, this Acknowledgement, any applicable contract or memorandum of understanding, clients of the AGO, or services provided by the AGO. All Users shall abide by and be aware of the following:

- Personal blogs shall contain clear disclaimers that the views expressed by the author in the blog are the author's alone and do not represent the views of the AGO;
- User shall refrain from discussions regarding employees and clients of the AGO on any social media or networking site;
- Social media activities shall not be conducted on AGO networks or while using the AGO's Internet;
- User's online presence may be linked to this Acknowledgement, any applicable related contract or memorandum of understanding, and the AGO. Be aware that the User's actions captured through images, posts, or comments should not include illegal, harassing, or other content that violates the law and/or the User's employer's or the AGO's policies or ethical requirements. Such conduct may lead to termination of the User's employment relationship with the AGO;
- AGO logos and templates shall not be used on personal blogs or for personal postings on social network sites; and
- Users engaging in chat rooms, blogging, tweeting, or other social media during non-working hours shall not reference or discuss information from the AGO or represent themselves as employees of, or spokespersons for, the Attorney General or the AGO.

IV. USER'S UNDERSTANDINGS

- User understands that any User who engages 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. User is responsible for obtaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
- User understands that the confidentiality and privileged nature of AGO files and information/data must be respected and protected. 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 information/data integrity. User also understands that the AGO has the right to remove or destroy unauthorized materials found on AGO networks and to terminate User's employment relationship with the AGO for breach of this Policy.
- 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 the User's activities and information may be released pursuant to a public records or discovery request.

- User understands that web browsers leave "footprints" that provide a record of all site visits. Access to, and use of, the Internet is not confidential and may be a public record.
- User understands that all Users and their employers will be held responsible and liable to the fullest extent of the law for actions while using the AGO's network resources, computers, and Internet.

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:

(VPN, AGO Domain Account, systems support, 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 Contract #:_____

AGO ITS Work Order Number: _____

AGO issued username: _____

AGO issued rights: _____

_____

_____

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

Name: _____ Title: _____

Signature: _____ Date: _____

Comments: _____

_____

_____

_____

_____

_____

_____