

Please read this policy carefully. It contains important information about your responsibilities and rules you must follow once you are granted access to the CLIENT computer facilities. Your signature indicates that you understand the terms of this policy. A copy of the signed policy will be kept on file.

CLIENT Computer/Information Usage Agreement

In consideration for accessing and using the CLIENT computer facilities, networks, Internet, Intranet or Extranet connections, electronic mail, licensed or developed software, software documentation or electronic data of any kind (hereafter referred to as "information"), I understand and agree to the following rules:

I shall use **information** and **computing resources** consistent with CLIENT's ethics policy or, in the absence of a CLIENT ethics policy, the Abator Business Conduct and Ethics policy.

I understand that computer passwords are confidential and should not be shared with, or used by, any other person.

At no time will I share or use another person's computer password.

I shall use care in protecting information from unauthorized access, misuse, theft, damage, destruction, modification or disclosure.

At no time shall I access, or attempt to access, any information without having the express authority to do so.

At no time shall I access, or attempt to access, any information in a manner inconsistent with the approved method of system entry.

At no time will I leave a workstation without first ensuring that I have properly secured the workstation from unauthorized access.

I understand that all information developed while on the job or while using CLIENT facilities or resources will be the exclusive property of the CLIENT.

I shall not copy, share, distribute, disclose, sublicense, modify, reverse engineer or sell any software licensed, developed or being evaluated by the CLIENT **unless** I have received prior written approval from the facility's MIS director to do so. At all times I shall use care to protect and keep such software strictly confidential in accordance with the license or any other agreement by the CLIENT.

The use of CLIENT software on non-CLIENT equipment is permitted only if I have received prior written approval from the facility's MIS director. If I require software to perform job functions off site, I must have prior written approval from the appropriate authority within the agency and the facility's MIS director.

I shall only use equipment or software owned, licensed or being evaluated by the CLIENT. I may not use personal or third-party equipment or software at CLIENT facilities **unless** I have received prior written approval from my supervisor and from the facility's MIS director. I understand that the LAN administrator must perform a virus scan on any software prior to installation. I understand that all software used on CLIENT computers will be procured properly through the appropriate CLIENT procedures.

I understand that the CLIENT reserves the right to monitor use of all CLIENT-provided equipment and information including, but not limited to, electronic mail, Internet and Intranet.

I understand that the CLIENT may conduct unannounced internal audits of software to monitor and assure compliance with CLIENT policy.

If I am found in violation of this Computer Use Policy, I may face disciplinary actions including reprimand, suspension, termination of employment or criminal or civil prosecution if the act is a violation of law.

I understand that this policy may be modified to reflect any changes in CLIENT policy or procedures. I will be notified in writing of any modifications and will be required to adhere to the modifications.

Virus, Malicious, Mischievous or Destructive Programming

Notwithstanding any other provision in this agreement to the contrary, provided the CLIENT has fully complied with its software security standards, if the CONSULTANT introduces a virus or malicious, mischievous or destructive programming into the CLIENT and has failed to comply with the CLIENT's software security standards and provided further that the CLIENT can demonstrate that the virus or malicious, mischievous or destructive programming was introduced by the CONSULTANT, the CONSULTANT shall be liable for any damage to any data and/or software owned or licensed by the CLIENT in the event a computer virus or malicious, mischievous or destructive programming is discovered to have originated from the CONSULTANT. In addition, the CONSULTANT shall be liable for any damages incurred by the CLIENT including, but not limited to, the expenditure of CLIENT funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that result from the CONSULTANT's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the CONSULTANT through appropriate firewalls and maintenance of anti-virus software and software security updates (such as operating systems security patches, etc.). In the event of destruction or modification of software, the CONSULTANT shall eliminate the virus, malicious, mischievous or destructive programming, restore the CLIENT's software, and be liable to the CLIENT for any resulting damages. CONSULTANT shall be responsible for reviewing CLIENT software security standards and complying with those standards.

CLIENT may, at any time, audit, by a means deemed appropriate by the CLIENT, any computing devices being used by CONSULTANT to provide services to the CLIENT for the sole purpose of determining whether those devices have anti-virus software with current virus signature files and the current minimum operating system patches or workarounds have been installed. Devices found to be out of compliance will immediately be disconnected and will not be permitted to connect or reconnect to the CLIENT network until the proper installations have been made.

CONSULTANT may use the anti-virus software used by the CLIENT to protect CONSULTANT's computing devices used in the course of providing services to the CLIENT. It is understood that the CONSULTANT may not install the software on any computing device not being used to provide services to the CLIENT, and that all copies of the software will be removed from all devices upon termination of this contract or any other agreement under which services are being provided.

CLIENT will not be responsible for any damages to CONSULTANT's computers, data, software, etc., caused as a result of the installation of CLIENT's anti-virus software or monitoring software on CONSULTANT's computers.

Neither the installation of the CLIENT's anti-virus software nor the installation of monitoring software will relieve the CONSULTANT of the liability requirements set out in this agreement.

For the purpose of this agreement, User's "Manager" is intended to mean the person recognized as being responsible for coordinating, overseeing, etc., user's contract relationship with the CLIENT.