

ACCEPTABLE USE POLICY (AUP)

<<insert date>>

Information Security Office
ENTER PRACTICE NAME HERE

Acceptable Use Policy (AUP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

TABLE OF CONTENTS

I.	Purpose	2
II.	Scope	2
III.	General Computer Use and Data Ownership Policy	2
IV.	Unacceptable Use	3
IV.I	System and Network Activities	3
IV.II	Email and Communication Activities.....	5
IV.III	Blogging and Social Media	5
IV.III	Reporting Software Malfunctions	6
V.	Enforcement, Auditing, Reporting	7

Revision History

Date of Change	Responsible	Summary of Change
September 2018	TTG SAS	TTG template revision v4

Acceptable Use Policy (AUP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

I. PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at **enter practice name here** ("the Practice"). These rules are in place to protect the employee and the Practice. Inappropriate use exposes the Practice to risks including virus attacks, compromise of network systems and services, and legal issues.

To comply with Written Information Security Program to ensure that plans are developed to establish appropriate and acceptable practices regarding the use of information resources.

II. SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct the Practice business or interact with internal networks and business systems, whether owned or leased by the Practice, the employee, or a third-party. All employees, contractors, consultants, temporary, and other workers at the Practice and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Practice policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at the Practice including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Practice.

III. GENERAL COMPUTER USE AND DATA OWNERSHIP POLICY

The Practice non-public, sensitive information stored on electronic and computing devices whether owned or leased by the Practice, the employee or a third party, remains the sole property of the Practice. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Information Security Policy*.

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Practice are the property of the Practice unless covered by a contractual agreement. Nothing contained herein applies to software purchased by Practice employees at their own expense.

You have a responsibility to promptly report the theft, loss or unauthorized disclosure of the Practice non-public, sensitive information.

You may access, use or share Practice non-public, sensitive information only to the extent it is authorized and necessary to fulfill your assigned job duties. For security and network maintenance purposes, authorized individuals within the Practice may monitor equipment, systems and network traffic at any time.

Acceptable Use Policy (AUP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Only computer hardware and software owned by and installed by the Practice is permitted to be connected to or installed on Practice equipment. Only software that has been approved for corporate use by the Practice may be installed on Practice equipment. Personal computers supplied by the Practice are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the Practice for home use. The Practice reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

It is the responsibility of all Practice personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted Practice office location, you should challenge them as to their right to be there. All visitors to Practice offices must sign in at the front desk. In addition, all visitors, excluding patients, **must wear a visitor/contractor badge**. All other personnel must be employees of the Practice. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

IV. UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the Practice authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Practice-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

IV.I System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Practice policy states that all computers will have the automatic screen lock function set to automatically activate upon **seven (7) minutes of inactivity**. Employees are not allowed to take any action which would override this setting.
2. Violations of the rights of any person or Practice protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Practice.

Acceptable Use Policy (AUP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Practice or the end user does not have an active license is strictly prohibited.
4. Accessing data, a server or an account for any purpose other than conducting Practice business, even if you have authorized access, is prohibited. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The Practice has access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, peer-to-peer ("P2P"), etc.).
 - a. **Exception:** Authorized information system support personnel, or others authorized by the Practice ISC, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
8. Using a Practice computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
9. Making fraudulent offers of products, items, or services originating from any Practice account.
10. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
11. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
12. Port scanning or security scanning is expressly prohibited without prior notification and express permission.

Acceptable Use Policy (AUP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

13. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
14. Circumventing user authentication or security of any host, network or account.
15. Introducing honeypots, honeynets, or similar technology on the Practice network.
16. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
17. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
18. Providing information about, or lists of, the Practice employees to parties outside the Practice.

IV.II Email and Communication Activities

When using Practice resources to access and use the Internet, users must realize they represent the Practice. Whenever employees state an affiliation to the Practice, they must also clearly indicate that *"the opinions expressed are my own and not necessarily those of the <insert practice name>"*. Questions may be addressed to the Information Security Coordinator ("ISC").

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within the Practice's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Practice or connected via the Practice's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

IV.III Blogging and Social Media

1. Blogging by employees, whether using the Practice's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the Practice's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the Practice's policy, is not detrimental to the

Acceptable Use Policy (AUP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

- Practice's best interests, and does not interfere with an employee's regular work duties. Blogging from the Practice's systems is also subject to monitoring.
2. The Practice's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Practice non-public, sensitive or proprietary information, trade secrets or any other material covered by the Practice's Confidential Information policy when engaged in blogging.
 3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the Practice and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the Practice's Non-Discrimination and Anti-Harassment policy.
 4. Employees may also not attribute personal statements, opinions or beliefs to the Practice when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the Practice. Employees assume any and all risk associated with blogging.
 5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, The Practice's trademarks, logos and any other Practice intellectual property may also not be used in connection with any blogging activity.

IV.III Reporting Software Malfunctions

Users should inform the appropriate Practice personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the Practice computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel or Practice ISO as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

Acceptable Use Policy (AUP)

Responsible Office: <<TBD>>

Effective Date: <<insert date>>

The ISC should monitor the resolution of the malfunction or incident, and report to Practice management the result of the action with recommendations on action steps to avert future similar occurrences.

V. ENFORCEMENT, AUDITING, REPORTING

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of Practice information resources access privileges, civil, and criminal prosecution. (**Note:** *Appropriate legal advisors and/or human resources representatives should review the policy and all of the procedures in use for policy enforcement. Some legal/human resources believe it is not necessary to include this section because all policy is enforceable. In fact, if it is included in one, it may be detrimental to the enforcement of other policies that do not include the section.*)
2. Practice Management is responsible for the periodic auditing and reporting of compliance with this policy. Executive Management will be responsible for defining the format and frequency of the reporting requirements and communicating those requirements, in writing, to Practice Management.
3. Exceptions to this policy will be considered only when the requested exception is documented and submitted to the Practice's ISC and designated Practice Management.