

## Acceptable Use Policy and Procedures

---

### Objectives

This policy establishes an outline for expected Sonsray employee behavior regarding the use of Sonsray's computer equipment. Signed access agreements include an acknowledgement that individuals have read, understood, and agreed to abide by the policy. These rules are in place to protect the Sonsray employee and Sonsray from unauthorized access to the Information Systems Network (ISN). Inappropriate use exposes Sonsray to risks including virus attacks, compromise of network systems and services, and legal issues.

---

### Policy Statement

The scope of this policy is applicable to all users of information technology resources connected to Sonsray's ISN. The systems are applicable whether owned or leased by Sonsray, the Sonsray employee, or third party. All Sonsray employees, contractors, consultants, temporary Sonsray employees, and other workers at Sonsray are responsible for exercising good judgment regarding appropriate use of information, electronic devices, removable media, and network resources in accordance with Sonsray policies and standards, and local laws and regulation. This policy applies to Sonsray employees, contractors, consultants, temporary Sonsray employees, and other workers at Sonsray including all personnel affiliated with third parties.

Sonsray has provided access to company electronic communications systems, networks, and devices, collectively with Sonsray employees referred to as "Authorized Users." These standards are the minimum acceptable use requirements. It is acceptable to implement measures that are more stringent than what is documented in the standards. Exceeding the minimum requirements does not necessitate a security exception. Where requirements cannot be met, a Security Exception must be filed, reviewed, and approved by IT Management. The exception request must describe compensating security controls. Exceptions to this policy are documented and can be found in the IT Ticketing System.

---

### Use and Ownership

Sonsray manages access in accordance with internal policy and best practices described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-14.

---

*Continued on next page*

## Acceptable Use Policy and Procedures, Continued

---

### Use and Ownership, continued

The following subsections outline the standards that constitute Sonsray's policy. Each Sonsray business system or group is bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy.

- Sonsray's proprietary information stored on electronic and computing devices whether owned or leased by Sonsray, the Sonsray employee, or a third party, remains the sole property of Sonsray.
- Sonsray personnel are to promptly report the theft, loss or unauthorized disclosure of Sonsray proprietary information.
- You may access, use, or share Sonsray proprietary information only to the extent it is authorized and necessary to carry out your assigned job duties.
- Sonsray employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet, otherwise, Sonsray employees should be guided by this Acceptable Use Policy on personal use. If there is any uncertainty, consult supervisor or manager.

For security and network maintenance purposes, authorized individuals within Sonsray's network may monitor equipment, systems, and network traffic at any time. Sonsray's IT Team reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Occasional personal use of the Internet is acceptable, but this use must be reasonable, not during your regular work hours. Employees may use their Internet facilities for non-business research or browsing during mealtime or outside of work hours, provided that they adhere to all Company policies, and do not negatively impact internet bandwidth performance. Incidental and occasional personal use of the corporate e-mail system is acceptable.

---

*Continued on next page*

## Acceptable Use Policy and Procedures, Continued

---

### Security

It takes a village to keep any business' network secure; and it is not just the IT team that is responsible for this.

- System level and user level passwords must comply with Sonsray's Access Control Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 4-hour for end users and 15 minutes for users with administrative rights.
- Using a Sonsray e-mail address to register for a newsgroup should be limited and restricted to newsgroups relation to the employees' work.
- Postings by Sonsray employees from a Sonsray e-mail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Sonsray, unless posting is in the course of business duties.
- Sonsray employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.
- Sonsray employees are not authorized to install software by themselves. If additional software is required, submit a help desk ticket.

---

*Continued on next page*

## Acceptable Use Policy and Procedures, Continued

---

### **Protecting Data and Sensitivity**

Sonsray 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 Sonsray authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Sonsray owned resources. This includes, but is not limited to copyright infringement, discrimination, and negative statements regarding other companies or Sonsray, or the communication of unlawful materials. Sonsray employees should assume that all communications and information accessible via the network are copyrighted. Plagiarism is prohibited.

The Company's Internet, e-mail technology and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, or other local jurisdiction in any material way. Use of any Company resources for illegal activity is grounds for immediate dismissal, and the Company will cooperate with any legitimate law enforcement investigation including 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.

---

### **Sample Unacceptable Use**

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

- Violations of the rights of any person or company 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 Sonsray.

---

*Continued on next page*

## Acceptable Use Policy and Procedures, Continued

---

**Sample  
Unacceptable  
Use, continued**

- 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 Sonsray, or the end user does not have an active license is strictly prohibited.
- Accessing Sonsray data, Sonsray systems, or a Sonsray account for any purpose other than conducting Sonsray business, even if you have authorized access, is strictly prohibited.
- Introduction of malicious programs into the network or system (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others is prohibited. This includes family and other household members when work is being performed remotely.
- Using a Sonsray's 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.
- Making fraudulent offers of products, items, or services originating from any Sonsray account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the Sonsray employee is not an intended recipient or logging into a system or account that the Sonsray 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.

---

*Continued on next page*

## Acceptable Use Policy and Procedures, Continued

---

**Sample  
Unacceptable  
Use, continued**

- Port scanning or security scanning is prohibited, unless by authorized IT Management.
- Executing any form of network monitoring which will intercept data not intended for the Sonsray employee's host unless this activity is a part of the Sonsray employee's normal job/duty.
- Circumventing user authentication or security of any Sonsray host, device, or account.
- Interfering with or denying service to any Sonsray user other than the Sonsray employee's host (for example, denial of service attack).
- Subscribing to list servers or distribution lists that are not directly related to your job.
- Addressing messages to everyone, rather than recipients who "need to know."
- Sending messages unnecessarily results in lower system and user performance.
- Except in an emergency, establishing settings or protocols which allow e-mails to be redirected to non-company e-mail servers or equipment without prior permission from IT Management.
- Not constructing messages in a professional and efficient manner.
- The exchange of proprietary information, trade secrets, or any other privileged, confidential, or sensitive information is restricted and monitored.
- The creation and exchange of advertisements, solicitations, chain letters and other unsolicited e-mail.

---

*Continued on next page*

## Acceptable Use Policy and Procedures, Continued

---

### Sample Unacceptable Use, continued

- The creation, storage, or exchange of information in violation of copyright laws.
  - 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 Sonsray Internet/Intranet/Extranet.
  - Providing information about, or lists of, Sonsray employees to parties outside of Sonsray.
  - Accessing chain letters, unauthorized advertising, websites involving gambling or pornographic content websites.
- 

### E-mail and Communication

When using Sonsray company resources to access and use the Internet, understand that you represent the company. Below are examples of unacceptable use of e-mail and communication.

- Sending unsolicited e-mail messages, including the sending of "junk mail," or other advertising material to any individuals
  - Any form of harassment via e-mail, telephone, texting, messaging, or paging, whether through language, frequency, or size of messages
  - Unauthorized use, or forging, of e-mail header information
  - Soliciting other e-mail addresses to harass or to collect replies
  - Creating or forwarding schemes of any type
  - Use of unsolicited e-mail originating from within Sonsray' ISN or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Sonsray, or connected via Sonsray network
  - Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam)
- 

*Continued on next page*

## Acceptable Use Policy and Procedures, Continued

---

### **Blogging and Social Media**

Sonsray must assign appropriate personnel who will oversee Sonsray social media accounts to be done in a professional and responsible manner.

Sonsray employees are prohibited from downloading and using personal, IM software (i.e. AOL Instant Messenger, Personal Skype, Facebook, Yahoo, MSN, Trillian, Twitter, etc.) to transmit IM via the public Internet. Sonsray employees are also prohibited from accessing any social networking sites (i.e. Facebook, My Space, Twitter, etc.), streaming media programs (i.e. Pandora, Spotify, etc.), feeds, material and content unless the subject matter being blogged or streamed is directly required for fulfilling their job responsibilities and approved by the Company's Senior Management. No streaming media sites are to be accessed nor are any streaming media programs or applications to be downloaded, installed and/or operated by end users for entertainment purposes on Company provided computers systems and/or networks.

Sonsray employees who engage in blogging, texting or social networking should be mindful that their messaging or postings, even if done off premises and while off-duty, could have an adverse effect on the Company's legitimate business interests. For example, the information posted could be the Company's trade secret or confidential business information. In addition, some readers may view the Sonsray employee as a de facto spokesperson for the Company.

---

*Continued on next page*



## Acceptable Use Policy and Procedures, Continued

---

**Reminders to Bloggers**

If a Sonsray employee's blogging, texting or social networking includes any information related to the Company:

- Make it clear to the readers that the views expressed are theirs alone and that they do not reflect the views of the Company.
- Do not defame or otherwise disparage the products or services of Sonsray, its Sonsray employees, partners, affiliates, customers, vendors, or competitors. In addition, customers should not be cited or identified without their approval.
- Do not use the Sonsray' logo, trademark, other intellectual property, or proprietary graphics, or any copyrighted materials.
- Do not disclose any confidential or other proprietary information about Sonsray, or that of any other person or company that may harm or tarnish the image, reputation, and/or goodwill of Sonsray and/or any of its Sonsray employees.
- Never post, publish or otherwise disclose information related to government contracts, specifically information classified as Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).
- Do not post a photo containing any Sonsray property.
- Do not post any photos of Sonsray employees at work or at any Company sponsored event.
- Do not engage in any blogging/social media while at work unless it is part of one's official job duties.
- Do not make any discriminatory, disparaging, defamatory, or harassing comments when blogging/social media or otherwise engaging in any conduct prohibited by Sonsray Nondiscrimination and Anti-Harassment policy.

---

*Continued on next page*

## Acceptable Use Policy and Procedures, Continued

---

### Reminders to Bloggers, continued

- Do not attribute personal statements, opinions, or beliefs to Sonsray when engaged in blogging. If you are expressing your beliefs and/or opinions in blogs, you may not, expressly, or implicitly, represent yourself as a Sonsray employee or representative of Sonsray.
- Follow all laws pertaining to the handling and disclosure of copyrighted or export controlled materials
- Do not use the following in connection with any blogging or social media activity:
  - Personally identifiable information
  - Sonsray trademarks
  - Sonsray logos
  - Any other Sonsray intellectual property

---

### Monitoring

All E-mails sent to or received from all Company equipment or services (including, but not limited to, all attachments of any kind) are the property of the Company. Sonsray employees have no right to privacy in any such messages. Accordingly, the Company may, at any time, view such E-mails, and may disclose the contents of them to any party, at its sole discretion. By utilizing the Company mail system, Company equipment or Company services, Sonsray employees explicitly consent to this policy and agree to abide by it.

---

*Continued on next page*

## Acceptable Use Policy and Procedures, Continued

---

### **Monitoring,** continued

The Company has software and systems in place that can monitor and record all Internet and e-mail usage. Sonsray employees should be aware that our security systems are capable of recording (for each user) each Internet website, each chat, electronic message, newsgroup or e-mail message, and each file transfer into and out of our internal networks, and the Company reserves the right to do so at any time. Any transmission of Company files must have express written permission from the Sonsray employee's department manager. Any violation of this policy is strictly prohibited. No Sonsray employee has a reasonable expectation of privacy in his or her Internet usage.

The Company periodically accesses, screens, and discloses use of the Internet system to determine whether Sonsray employees are violating any applicable policies. The IT Team may review Internet activity and analyze usage patterns and may choose to publicize this data to assure that the Company's Internet resources are devoted to maintaining the highest levels of productivity.

In addition, the Company reserves the right to inspect all files stored in private areas of the network to assure compliance with this policy. Such inspection includes materials sent over and received from the Internet. Sonsray employees have no ownership or privacy expectations regarding such data. E-mail is a resource made available by the Company and is provided for use as a business communication tool. The Company reserves the right, at its discretion, to monitor any Sonsray employee's E-mail account for any reason. These reasons may include monitoring Sonsray employee performance, compliance with this policy, compliance with any applicable laws and industry regulations, and where there is a reasonable suspicion of activities that may violate this policy.

---

### **Loss or Theft**

The loss or theft of any company-owned equipment/devices or any devices which contain company or Sonsray data must be reported to the IT Team immediately.

---

*Continued on next page*

## Acceptable Use Policy and Procedures, Continued

---

**Enforcement**

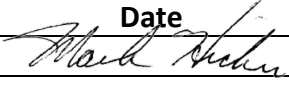
All Sonsray employees are responsible for compliance with this policy and associated guidelines as a condition of employment, contract, or practice at Sonsray. A statement acknowledging understanding of these policies and pledging compliance is signed by all users of information at the beginning of their association with Sonsray and/or prior to being granted access to any computer resources.

If a Sonsray employee is found violating a policy, a warning is given to the individual and recorded in the Sonsray employee’s personnel file. Further failure to comply may result in disciplinary action up to and including termination of employment or revocation of privileges.

---

**Revision Control History**

Below lists the Revision History for this document.

Revision Date	Revised By	Revision Status	Executive Approval, Date
2/15/2023	Rachelle McKenzie	New	

8/17/2023

---