**Acceptable Use Policy Template**

*Use of Template*

*This document covers most aspects of industry-standard Acceptable Use Policies. It should be thoroughly reviewed to decide what applies to your organization, as each organization varies in structure. Areas that are irrelevant or not enforced should be removed from your policy. An example would be the sections on blogging/social media or the section on password-protected lock screen.*

# **Purpose**

This policy aims to outline the acceptable use of computer equipment and other electronic devices at <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to cyber risks, including virus attacks, ransomware, compromise of network systems and services, data breach, and legal issues.

1. **Scope**

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

This policy applies to employees, contractors, consultants, temporaries, and other workers at <Company Name>, including all personnel affiliated with third parties. This policy applies to all equipment owned or leased by <Company Name>.

# **Policy**

# **3.1 General Use and Ownership**

# 3.1.1 - <Company Name> proprietary information stored on electronic and computing devices, whether owned or leased by <Company Name>, the employee or a third party, remains the sole property of <Company Name>. You must ensure through legal or technical means that proprietary information is protected.

# 3.1.2 - You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of <Company Name> proprietary information.

# 3.1.3 - You may access, use, or share <Company Name> proprietary information only to the extent authorized and necessary to fulfill your assigned job duties.

# 3.1.4 - 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/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

# 3.1.5 - For security and network maintenance purposes, authorized individuals within <Company Name> may monitor equipment, systems, and network traffic anytime.

# 3.1.6 - <Company Name> reserves the right to audit networks and systems periodically to ensure compliance with this policy.

**3.2 Security and Proprietary Information**

* 3.2.1 - All mobile and computing devices that connect to the internal network must comply with <Company Name>’s requirements..
* 3.2.2 - System-level and user-level passwords must comply with the organization’s password policy. Providing access to another individual, deliberately or through failure to secure its access, is prohibited.
* 3.2.3 - All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
* 3.2.4 - Employee postings from a <Company Name> email address to newsgroups or other online platforms should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name> unless posting is during business duties.
* 3.2.5 - Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

**3.3 Unacceptable Use**

* The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services).
* Under no circumstances is an employee of <Company Name> authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing <Company Name>-owned resources.
* The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

**3.3.1 System and Network Activities**

* The following activities are strictly prohibited, with no exceptions:
1. 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 <Company Name>.
2. 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 <Company Name> or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting <Company Name> business, even with authorized access, is prohibited.
4. 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 before the export of any material that is in question.
5. Introducing malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
6. Revealing your account password/passphrase to others or allowing the use of your account by others. This includes family and other household members when work is done at home.
7. Using a <Company Name> computing asset to actively procure or transmit material that violates sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any <Company Name> account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. 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, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
11. Port or security scanning is expressly prohibited unless prior notification to the Infosec Team is made.
12. Executing any form of network monitoring that will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the <Company Name> network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. 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.
17. Providing information about, or lists of, <Company Name> employees to parties outside <Company Name>.

**3.3.2 Email and Communication Activities**

* When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company." Questions may be addressed to the IT Department
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, text, 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 <Company Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>'s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

 **3.3.3 Blogging and Social Media**

1. Blogging or posting to social media platforms by employees, whether using <Company Name>’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 <Company Name>’s systems to engage in blogging or other online posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>’s policy, is not detrimental to <Company Name>’s best interests and does not interfere with an employee's regular work duties. Blogging or other online posting from <Company Name>’s systems is also subject to monitoring.
2. <Company Name>’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets, or any other material covered by <Company>’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 <Company Name> 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 <Company Name>’s Human Resource policies.
4. Employees may also not attribute personal statements, opinions, or beliefs to <Company Name> 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 <Company Name>. Employees assume any and all risks associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, <Company Name>’s trademarks, logos, and any other <Company Name> intellectual property may also not be used in connection with any blogging or social media activity

**4. Policy Compliance**

* 4.1 - Compliance Measurement

The Infosec Team will verify compliance with this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

* 4.2 - Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

* 4.3 - Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**5. Definitions and Terms**

The following definition and terms can be found in the SANS Glossary at: <https://www.sans.org/security-resources/glossary-of-terms/>

* Authentication - is the process of confirming the correctness of the claimed identity.
* Brute Force - a cryptanalysis technique or attack method involving an exhaustive procedure that tries all possibilities, one by one.
* Denial of Service - the prevention of authorized access to a system resource or the delaying of system operations and functions.
* Internet - a term to describe connecting multiple separate networks together.
* Intranet - a computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.
* Proprietary Information - is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.
* Ransomware - A type of malware that is a form of extortion. It encrypts a victim's hard drive and denies them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.
1. **Revision History**

| Date of Change | Responsible | Summary of Change |
| --- | --- | --- |
|  |  |  |
|  |  |  |