Acceptable Use Policy

Last Update Status: Updated June 2022

1. Overview

Infosec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to F1 TEAM's established culture of openness, trust and integrity. Infosec is committed to protecting F1 TEAM's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of F1 TEAM. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every F1 TEAM employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at F1 TEAM. These rules are in place to protect the employee and F1 TEAM. Inappropriate use exposes F1 TEAM to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct F1 TEAM business or interact with internal networks and business systems, whether owned or leased by F1 TEAM, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at F1 TEAM and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with F1 TEAM policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at F1 TEAM, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by F1 TEAM.

4. Policy

4.1 General Use and Ownership

4.1.1 F1 TEAM proprietary information stored on electronic and computing devices whether owned or leased by F1 TEAM, the employee or a third party, remains the sole property of F1 TEAM. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of F1 TEAM proprietary information.

4.1.3 You may access, use or share F1 TEAM proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 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.

4.1.5 For security and network maintenance purposes, authorized individuals within F1 TEAM may monitor equipment, systems and network traffic at any time, per Infosec's *Audit Policy*.

4.1.6 F1 TEAM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a F1 TEAM email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of F1 TEAM, unless posting is in the course of business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 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 F1 TEAM authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing F1 TEAM-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.

4.3.1 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 F1 TEAM.
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 F1 TEAM or the end user does not have an active license is strictly prohibited.
3. Making fraudulent offers of products, items, or services originating from any F1 TEAM account.
4. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
5. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
6. 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.
7. Circumventing user authentication or security of any host, network or account.
8. Introducing honeypots, honeynets, or similar technology on the F1 TEAM network.
9. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
10. Providing information about, or lists of, F1 TEAM employees to parties outside F1 TEAM.

4.3.2 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 Human Resources

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.

4.3.3 Blogging and Social Media

1. F1 TEAM's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any VLMT confidential or proprietary information, trade secrets or any other material covered by VLMT's Confidential Information policy when engaged in blogging.
2. Employees may also not attribute personal statements, opinions or beliefs to F1 TEAM 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 F1 TEAM. Employees assume any and all risk associated with blogging.
3. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, F1 TEAM's trademarks, logos and any other F1 TEAM intellectual property may also not be used in connection with any blogging activity

5. Policy Compliance

5.1 Compliance Measurement

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

5.2 Exceptions

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

5.3 Non-Compliance

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

6. Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy

7. Definitions and Terms

- none

8. Revision History

Date of Change	**Responsible**	**Summary of Change**
June 2020	Human Resources	Updated and converted to new format
July 1,2022	Human Resources	New season