**Acceptable Use Policy**

# Overview

Infosec’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Team 18’s established culture of openness, trust and integrity. Infosec is committed to protecting Team 18'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 Team 18. 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 Team 18 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.

# Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Team 18. These rules are in place to protect the employee and Team 18. Inappropriate use exposes Team 18 to risks including virus attacks, compromise of network systems and services, and legal issues.

# Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Team 18 business or interact with internal networks and business systems, whether owned or leased by Team 18, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Team 18 and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Team 18 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 Team 18, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Team 18.

# Policy

## General Use and Ownership

## Team 18 proprietary information stored on electronic and computing devices whether owned or leased by Team 18, the employee or a third party, remains the sole property of Team 18. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

## You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Team 18 proprietary information.

## 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.

## For security and network maintenance purposes, authorized individuals within Team 18 may monitor equipment, systems and network traffic at any time, per Infosec's *Audit Policy*.

## Team 18 reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

## Company information may not be placed onto non company nor personal devices without proper prior authorization. This includes discussion over emails that are not governed by Team 18.

* 1. **Security and Proprietary Information**
     1. All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.
     2. Postings by employees from a Team 18 email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Team 18, unless posting is in the course of business duties.
     3. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.
  2. **Unacceptable Use**

The following activities are, in general, prohibited.

Under no circumstances is an employee of Team 18 authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Team 18-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.

* + 1. Email and Communication Activities

When using company resources to access and use the Internet, users must realize theyrepresent 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 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 Team 18's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Team 18 or connected via Team 18's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
   * 1. Blogging and Social Media
8. Usage of social media platforms on company mobile and computing devices are not authorized at any time.
9. Discussion of company topics that may or may not harm the integrity of company information are not authorized to be posted on any social media platforms.

Policy template from: https://www.sans.org/security-resources/policies/general#acceptable-use-policy