Acceptable Use Policy

1. Overview

Infosec Team’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to FinServCo’s established culture of openness, trust and integrity. FinServCo is committed to protecting FinServCo'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, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of FinServCo. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every FinServCo 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.

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

2. Policy

2.1 General Use and Ownership

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

2.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of FinServCo proprietary information.

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

2.1.4 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.

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

2.1.6 FinServCo reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.1.7 All employees are required to report violations of this policy immediately to their infosec Team or to their supervisors. Reporting can be made by email to [infosec@finservco.com] or alternatively through the internal reporting platform. The confidentiality of the reporting party should be fully maintained.

2.2 Security and Proprietary Information

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

2.2.2 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.

2.2.3 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.

2.2.4 Postings by employees from a FinServCo 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 FinServCo, unless posting is during business duties.

2.2.5 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

2.2.6 All employees are required to participate in the annual security training sessions. These sessions cover current cybersecurity threats, responsibilities under this policy, and prevention techniques. Training sessions will be scheduled by HR, attendance is mandatory to access company systems.

2.2.7 To protect sensitive data, data encryption must be utilized for all proprietary information stored on company owned devices and transmitted over public or external networks. Guidelines on implementing appropriate encryption methods is available in the Data Protection Standard.

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

2.3.1 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 FinServCo.
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 FinServCo 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 FinServCo business, even if you have 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 prior to export of any material that is in question.
5. Introduction of 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 use of your account by others. This includes family and other household members when work is being done at home.
7. Using a FinServCo 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.
8. Making fraudulent offers of products, items, or services originating from any FinServCo 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 scanning or security scanning is expressly prohibited unless prior notification to the Infosec Team is made.
12. 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.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the FinServCo 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, FinServCo employees to parties outside FinServCo.

2.3.2 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 FinServCo's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by FinServCo or connected via FinServCo's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.3.3 Blogging and Social Media

1. Blogging or posting to social media platforms by employees, whether using FinServCo'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 FinServCo'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 FinServCo's policy, is not detrimental to FinServCo's best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from FinServCo's systems is also subject to monitoring.
2. FinServCo's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any FinServCoconfidential or proprietary information, trade secrets or any other material covered by FinServCo'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 FinServCo 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 FinServCo's *Non-Discrimination and Anti-Harassment* policy.
4. Employees may also not attribute personal statements, opinions or beliefs to FinServCo 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 FinServCo. 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, FinServCo's trademarks, logos and any other FinServCo intellectual property may also not be used in connection with any blogging or social media activity.

2.3.4 Examples of Prohibited Behavior

1. Prohibited Behavior includes, but are not limited to, the use of derogatory language, engaging in discriminatory actions, disseminating sexually explicit material, and making threats.

2.3.5 Disciplinary Actions for Policy Violation

1. Violations of this policy will result in disciplinary action,

3. Policy Compliance

3.1 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.

3.2 Exceptions

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

3.3 Annual review

This policy will be updated and reviewed annually to ensure it remains effective and aligned with industry standards and regulations. Next review date is [13/4/2025].

4. Related Standards, Policies and Processes

4.1 Access to Related Documents

All related documents, including the Data Classification Policy, Data Protection Standard, and social media Policy, are available on the corporate intranet at [insert URL] or can be obtained by contacting the Infosec Team.

5. Support and Resources

5.1 Contant Information

For questions about this current policy or security practices, please contact the infosec team at [incofsec@finservco.com].

5.2 Educational resources

Additional training materials and resources on information security are available on the employee training portal at [example.com]. External courses recommended by the infosec team can also be found here.