Acceptable Use Policy

Information Systems

DOCUMENT SUMMARY:

AUTHOR	INFORMATION SECURITY MANAGER
REVIEWED BY	CIO/CISO
CURRENT VERSION	2.0
DATE OF CURRENT VERSION	04-03-2020
DOCUMENT REFERENCE NO.	SFO-AUP-POL-001
DOCUMENT TYPE	POLICY
DOCUMENT STATUS	FINAL
DOCUMENT CIRCULATION	NEED BASED CIRCULATION ONLY
OWNER	INFORMATION SECURITY MANAGER
APPROVED BY	MANAGING DIRECTOR

DOCUMENT AMENDMENT RECORD

CHANGE NO.	DATE	PREPARED BY	BRIEF EXPLANATION
0.1	05-08-2018	Acceptable Use Policy Information Systems	Version 1.0
1.0	04-03-2020	Acceptable Use Policy Information Systems	Version 2.0

Acceptable Use Policy – Information Systems

1.0 Purpose and Applicability

This Acceptable Usage Policy covers the security and use of all information and IT equipment of SFO Technologies Private Limited, A NeST Group Company (hereafter referred to as 'SFO'). It also includes the use of email, internet, vpn and remote access, voice and mobile IT equipment including Smartphones with or without Camera. This policy applies to all employees, consultants, outsourced employees and contractors (hereafter referred to as 'individuals') of SFO.

This policy applies to all information, in whatever form, relating to SFO's business activities worldwide, and to all information handled by SFO relating to other organisations with whom it deals. It also covers all sites and divisions and IT and information communications facilities operated by SFO or on its behalf including its subsidiary companies and sister concerns under NeST group.

2.0 Computer Access Control – Individual's Responsibility

Access to the SFO IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the SFO IT systems.

All Data classified as Highly Sensitive must be handled only by the authorised personnel and the confidentiality protocols must be followed as detailed in the Data Classification Policy.

2.1. Individuals must not:

a) Allow anyone else to use their user ID/token and password on any SFO IT system.
b) Leave their user accounts logged in at an unattended and unlocked computer.
c) Use someone else's user ID and password to access SFO IT systems.
d) Leave their password unprotected (for example writing it down).
e) Perform any unauthorised changes to SFO IT systems or information.
f) Attempt to access data that they are not authorised to use or access.
g) Exceed the limits of their authorisation or specific business need to interrogate the system or data.
h) Connect any non-SFO device to the SFO network or IT systems.

i) Store SFO data on any non-authorised SFO equipment or data storage media like USB, CD Drives, SD Cards, Mobile Phones, Tabs, Digital Cameras etc.
j) Give or transfer SFO data or software in any format or media to any person or organisation outside SFO without the authority of SFO.
k) Attempt to use the features of smartphones or new electronic gadgets like the google glass (and similar innovative new technology) for data collection or image capture.
l) Carry devices or any equipment into areas marked as 'restricted' 'or prohibited'.
m) Carry any equipment capable of image capture into photography prohibited areas and use them.

3.0 Internet and email Conditions of Use

Use of SFO internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to SFO in any way, not in breach of any term and condition of employment and does not place the individual or SFO in breach of statutory or other legal obligations and it shall not have any kind of liability to the organisation.

All individuals are accountable for their actions on the internet and email systems.

3.1 Individuals must not:

a) Use the internet or email for the purposes of harassment or abuse.
b) Use profanity, obscenities, or derogatory remarks in communications.
c) Access, download, send or receive any data (including images), which SFO considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
d) Use the internet or email to make personal gains or conduct a personal business.
e) Use the internet or email to gamble.
f) Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
g) Click on a link sent by email from an untrustworthy source and fall prey to Phishing or engage in identity theft.
h) Introduce and/or distribute computer viruses, worms, Trojan horses or other malicious code
i) Introduce and/or distribute pornography or adult related content or offering any escort services
j) Promote or facilitate violence, hate or terrorist activities
k) Infringe the intellectual property or other proprietary rights of others

l) Place any information on the Internet that relates to SFO, alter any information about it, or express any opinion about SFO, unless they are specifically authorised to do this.

m) Send unprotected sensitive or confidential information externally.
n) Forward SFO mail to personal (non-SFO) email accounts (for example a personal Hotmail or Gmail accounts).
o) Must not engage in any social media posts, blogs that may harm or tarnish the reputation of SFO.
p) Make official commitments through the internet or email on behalf of SFO unless authorised to do so.
q) Download copyrighted material such as music media files, film and video files (not an exhaustive list) without appropriate approval.
r) In any way infringe any copyright, database rights, trademarks or other intellectual property.
s) Download any software from the internet without prior approval of the IT Department.
t) Connect SFO devices to the internet using non-standard connections.
u) Must not violate any general data protection policy of the Country, State and Central Governments.

4.0 Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, SFO enforces a clear desk and screen policy as follows:

a. Personal or confidential business information must be protected using security features provided for example secure print on printers.
b. Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
c. Care must be taken to not leave confidential material on printers or photocopiers.
d. All business-related printed matter must be disposed of using confidential waste bins or shredders.

5.0 Working Off-site / Working from Home

It is accepted that laptops and mobile devices will be taken off-site during duty travel. In exceptional cases work from home and remote working is permitted subject to the recommendation of the Departmental Head and approved by the Unit Head. Individuals that participate in remote working arrangements are expected to satisfy all job responsibilities, meet performance expectations, and follow all policies/procedures that govern their employment. Using a virtual private network

(VPN) and creating a secure tunnel is the approved remote access method to access SFO's internal networks, systems, and data.

5.1 The following controls must be applied by the individual:

a. Working away from the office must be in line with SFO remote working policy.
b. However, using a VPN to access internal resources comes with individual responsibilities to uphold network security, as well as to safely and equitably use company resources.
c. All Equipment such as desktops laptops and mobile devices must be installed with anti-virus/malware, firewalls, and application/Security/OS patches should be updated as necessary.
d. Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
e. Laptops must be carried as hand luggage when travelling.
f. Information must be protected against loss or compromise when working remotely (for example at home or in public places).
g. Laptop encryption must be used.
h. Particular care must be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.
i. Privacy enhancement with the use of display protection filters should be used when sensitive data is accessed especially in public places.
j. Home Wireless networks, Hotspots must be securely configured utilizing strong encryption (i.e. WPA2 with a strong pre-shared key).
k. Do not connect to open and insecure wireless networks or internet connections.
l. All individuals must be conscious that they are handling the IT Assets of the company but also the intellectual property of the company and the loss of which will result in substantial loss and goodwill of the company.

6.0 Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives are not permitted to use in company premises. If under any circumstance, the use of this is required special approval shall be taken from the department head and from IT department. Data transfer using smartphones is strictly prohibited and smartphones are generally classified as untrusted except with approved exceptions.

7.0 Mobile Phones

Individuals who are provided with company SIM Cards shall ensure that it is used only for official purpose and shall be available on call at any time. Such sim cards

shall not be used for personal use such as WhatsApp, Facebook, Chatting, Facetime and other social media platforms which will keep the phone unavailable for official purpose. The usage of mobile phones shall be strictly in areas permitted for use. Company reserves the right to track, monitor and record the usage of the company provided sim card.

8.0 Software

Employees must use only software that is authorised by SFO on SFO computers and end user devices. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on SFO computers must be approved and installed by the SFO IT department.

Individuals must not:

a) Store personal files such as music, video, photographs or games on SFO IT equipment.

9.0 Viruses

The IT department has implemented centralised, automated virus detection and virus software updates within SFO. All devices have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

a) Remove or disable anti-virus software.
b) Attempt to remove virus-infected files or clean up an infection, other than by the use of approved SFO anti-virus software and procedures.

10.0 Video Conferencing, Telephony (Voice) Equipment Conditions of Use

Use of SFO voice / video equipment is intended for business use. All users of solutions like Zoom, Skype, Microsoft Teams, Webex etc shall make sure that IT Security Guidelines are strictly followed. Individuals must not use SFO video / voice facilities for sending or receiving private communications on personal matters. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

a) Use SFO's video / voice for conducting private business.
b) Make hoax or threatening calls to internal or external destinations.
c) Record the calls or video confernece meeting unless its pre-approved.

d) Conduct video calls from home or off-site premises if the environment is not free of disturbances and distractions.

11.0 Actions upon Termination of Contract

All SFO equipment and data, for example laptops and mobile devices including telephones, Sim Cards, smartphones, data connection devices, USB memory devices and CDs/DVDs, or any other given to the employee must be returned to SFO at termination of contract.

All SFO data or intellectual property developed or gained during the period of employment remains the property of SFO and must not be retained beyond termination or reused for any other purpose.

Email communications and network access will be disabled immediately upon termination of contract.

12.0 Monitoring and Filtering

All data that is created and stored on SFO computers is the property of SFO and there is no official provision for individual data privacy, however wherever possible SFO will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. SFO has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the prevailing cyber laws and e-security of India, IT ACT 2000, ISO 27001, NIST guidelines will regulate the governance steps.

13.0 Jurisdiction

In the event of any dispute regarding this policy, the court of jurisdiction will be Ernakulam, Kerala, India.

I will make every effort to report any suspected breaches of security policies coming to my notice to the management and to the IT department.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with SFO disciplinary procedures. I understand that my services can be suspended or terminated with or without notice upon any violation of this policy. Any violations may also result in the immediate suspension or termination of my account and company can proceed with legal recourse. I also understand that I am personally responsible for the proper handling and upkeep of the company provided assets assigned to me and I will be responsible for the damage caused to the company by my omissions.