Safex Group

Acceptable Usage Policy

SURESH
01/04/23

S.NO	Topic	Page No.
1	Document Control	3
2	Purpose	4
3	Scope	4
4	Terms & Definition	4
5	Policy 5.1 Information Handling 5.2 Clear Desk & Clear Screen Policy 5.3 Access Control 5.4 Password Usage 5.4.1 Password Change 5.4.2 Password Transmission 5.4.3 Password Storage 5.5 Laptop & Desktop Usage 5.6 Mobile Media Usage 5.7 Email Usage 5.8 Internet Usage 5.9 Printer Usage 5.10 Document & Record Usage 5.11 Removable Media Usage 5.12 Unacceptable Usage 5.12.1 System and network activities 5.12.2 Photography	4 4 5 5 6 6 7 7 7 9 9 10 11 11 12 12 12 14
6	Work From Home Guidelines	14
7	Enforcement (Policy Violation)	15
8	Document Reference	16

Safex Group

Acceptable Usage Policy

1. Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Acceptable Usage Policy
2.	Document Code	ITAUP01
3.	Date of Release	01-04-2023
4.	Document Version No.	1.1
5.	Document Owner	Safex Group
6.	Document Author(s)	Suresh Yadav (AVP IT)
7.	Document Approver	Piyush Jindal (Group Director)

Document Update Summary

Version No.	Revision Date	Nature of Changes	Date Approval
1	28-03-2023	Review	01-04-2023
2			
3			

Suresh
01/04/23

2. Purpose

The purpose of this policy is to outline the acceptable usage of information and information processing systems of Safex Group. Adherence to the standards of this policy would reduce any potential misuse of information processing facilities of Safex Group.

3. Scope

The objective of this policy is to restrict or guide users on the do's & don'ts of information systems usage both within and outside of Safex Group.

4. Terms & Definition

For the purposes of this document, the following terms and definitions apply.

User	*A User is an individual who has access to the information and information processing facilities of Safex Group and uses it for their day-to-day activities.*
Asset	*Anything that has value to the organisation. Assets generally include hardware (e.g., servers and switches), software (e.g., mission critical applications and support systems)*
Information Asset	*An information asset is any information or information processing facility that has value to the organisation such as system, service, or infrastructure, or any physical location that houses these things. It can be either an activity or a place.*
IPR – Intellectual Property Rights	*Intellectual Property Rights – The legal rights of a person or company has to the ownership of their ideas, designs, and inventions, including copyrights, patents, and trademarks*

5. Policy

5.1. Information Handling

Users shall ensure that all information assets regardless of its form (electronic or physical) are classified appropriately to avoid loss of confidentiality, integrity, and availability of the information.

Users shall ensure that information assets are maintained at their defined classification level during the entire retention period even when used from home or anywhere outside office premises.

Users shall ensure that all information assets are labelled and stored securely with appropriate protection measures to avoid unauthorised access.

Users shall ensure that all information assets are distributed or transferred on a "need to know" basis, taking into consideration adequate protection measures.

Users shall ensure that all information assets are disposed securely in accordance with their classification and retention schedule.

Users shall inform the Information security Team or the manager/head of their department in case of any non-compliance to the above information handling requirements.

5.2. Clear Desk & Clear Screen Policy

Users shall ensure that they lock the computer terminals before leaving their desk during working hours.

Users shall ensure that they log out of all applications at the end of their working hours.

Users shall ensure that they shut down the computer terminals before leaving for the day.

Users shall use only Safex Group authorised screensavers and desktop wallpapers in their respective workstations.

Users shall ensure that sensitive information assets are securely maintained around their desks to avoid any unauthorised views.

Users shall ensure that all paper documents and electronic media are stored in locked cabinets or other secure storage areas before leaving for break or end of the day.

Keys to secure storage shall be held by authorised personnel. At no point shall a key to secure storage be left in or near the secure storage area.

Users shall ensure that they protect the incoming and outgoing postal mails etc. and do not leave them unattended around the facility.

Users shall ensure that they do not leave any paper documents unattended around photocopiers, scanners, or printing facilities.

Users shall ensure that the documents containing sensitive or classified information shall be removed from printers immediately.

5.3. Access Control

Users shall use their unique user credentials to access any kind of information processing facilities.

Users shall refrain from accessing information processing facilities with user credentials of other employees or affiliates.

Users shall follow the secure log on process of the applications and shall not try to bypass the process in any manner.

Users shall comply with all kinds of logon banners or warning notices that pop up during the secure logon to information systems.

Users shall obtain necessary approvals from the concerned owners of the system for different access privilege levels required on the information systems.

Users shall maintain their privilege levels on the information system on a "need to know" basis and comply with defined "least access privilege" principle.

Users shall not try and escalate their privilege levels on any information system and warn other employees or affiliates found doing the same.

Users shall maintain their exclusive access privileges on information processing facilities by not allowing anyone else to operate from their account.

Users shall refrain from using any special computer program or software that can override system or application controls.

Users shall follow and abide by the defined HR clearance procedure to revoke their access rights from information processing systems during end of tenure with Safex Group.

Users shall promptly report any incident that may violate the access control policy of Safex Group.

5.4. Password Usage

Users shall maintain confidentiality of all their logical accounts through good password management.

Users shall not share their passwords with anyone inside or outside the organisation.

Users shall be held accountable for all activities originating from their logical accounts.

Users shall not keep their passwords openly lying on desks, pasted on the computer screen, or stored in any other physical manner which can be easily viewed by others.

Users shall exercise extreme care and due diligence while using passwords in presence of others or in public places etc.

Users shall always choose passwords that are easy to remember but still difficult to guess by any adversary. Simple passwords such as dictionary words, person's name, person's date of birth, pet names etc. shall not be used.

Users shall choose passwords that meet the complexity requirements of the Password Policy & Standards of Safex Group. (Attached)

Users shall avoid using the same passwords for all information processing systems.

Users shall be aware of the general methods of password stealing such as phishing, social engineering, shoulder surfing etc.

5.4.1 Password Change

All information processing systems shall enforce users to change their passwords at least every 90 days.

All information processing systems shall restrict users from reusing the previous 03 passwords.

A proper log of all changes to system accounts or system level passwords has to be maintained by the application owner. The log shall contain the following details, but not limited to Date of Change & Name of the employee who changed the password & Reason for Change.

Password (s) shall be immediately changed in cases where a user account is compromised, or instances of data leakage are detected or suspected.

When an employee leaves the organisation, his/her user account(s) shall be immediately disabled, or password(s) changed.

5.4.2 Password Transmission

Passwords and related information shall always be communicated in a secure manner, without leaving any opportunities for unauthorised disclosure.

All information processing systems shall transmit passwords over the network in an encrypted form.

Administrators should avoid communicating passwords over the phone to the extent possible. When required to communicate passwords over the phone, appropriate measures have to be taken to ensure that the passwords are communicated only to the intended user.

Passwords shall never be printed in any form for transmission purposes.

5.4.3. Password Storage

If the user account is inactive for more than 90 days, the account will be disabled. The same can be activated upon request to the IT department by the personnel and due authorization by their reporting manager.

All information processing systems, wherever technically possible, shall store the passwords in non-reversible encrypted form.

All information processing systems shall maintain a particular password in active status only for a predefined period.

Information processing systems, wherever possible, shall disable the use of the "Remember password" feature.

Passwords shall not be stored in a form that can be subjected to unauthorised views e.g., written and openly kept on desks, pasted on computer screens with the help of post-aids etc.

System level administrative passwords that cannot be created and managed by a password management system shall be documented through encrypted excel format.

All system level administrative password requests shall be authorised by the IT Head.

The safe custodians shall release the password in a secure manner and directly to the requestor.

5.5 Laptop & Desktop Usage

Users shall ensure that they use only official laptops and desktops provided by Safex Group for their day-to-day activities at office.

Users shall get authorization from the information security team for using their personal laptops or PDAs to connect to the official network and/or for carrying out their official tasks.

Users will be responsible for the security of Safex Group laptops & desktops and will take adequate measures to ensure its physical and logical security. If any damage occurs to a company's assets due to negligence of employees, he/she will be held liable to bear the cost of damage at the discretion of management.

Users shall not install, update, or change any hardware, operating system, application or software on Safex Group laptops or desktops apart from the one specifically approved by the IT division of Safex Group.

Users shall not try to change any configuration settings of hardware, operating system, application, or software installed in Safex Group official laptops or desktops.

Users shall refrain from installing or using any unlicensed operating system, application or software in Safex Group official laptops or desktops without proper authorization.

Users shall avoid storing intellectual property of Safex Group such as software codes, router/switch configuration etc. in their personal laptops or desktops.

Users shall not share Safex Group laptops or desktops with other employees or unauthorised personnel.

Users shall not allow anyone to take away Safex Group laptops or desktops except for officials authorised by the IT division.

Users shall not leave the laptops unattended in public places or while travelling.

Users shall use a lock and key mechanism to prevent the theft of laptops in their absence.

Users shall ensure that the antivirus software is operational in their laptops or desktops.

Users shall not try and disable the anti-virus agent installed in their laptops or desktops

Users shall not try and disrupt the auto scan scheduled on Safex Group laptops or desktops. If the scan is affecting system performance, users shall report the issue through IT Support Desk itsupport@safexchemicals.com.

Users shall promptly report any cases of failure in automatic cleaning up of a virus, spyware, malware etc. through IT Support Desk.

Users shall promptly report any signs of a virus outbreak or repeated occurrence of a virus to the concerned IT division through IT Support Desk.

Users shall immediately report any theft of their official laptops or desktops through IT Support Desk.

Users shall request for any changes in the hardware, operating systems, application, or software installed in their official desktops or laptops through IT Support Desk.

When external visitors come with portable computing equipment, as far as possible they must be restricted from connecting it into the Safex Group network. However, if their job demands that they do so, they shall be allowed to do so only after approval by the Information Security Officer. The machine must be scanned for viruses before connecting into the network. If possible, they must be put on to secured subnets so that they do not get into the Safex Group LAN. Their network access privileges must be restricted.

All laptops shall have two profiles set on them – The user must always use the network profile while s/he is connected to Safex Group network. The other profile is used by the Administrators. The user of the laptop will be given admin privileges on the laptop which shall be exercised only when absolutely required.

5.6 Mobile Media Usage

Users shall ensure that they make use of officially provided USB storage devices and external hard drives to store official information.

Users shall refrain from using their personal USB devices or external hard drives to store official information.

Users shall make use of appropriate mechanisms approved by the IT Department to secure all information in mobile media devices.

Users shall regularly back up their information on the SVN/File server provided by the IT Department.

Users shall immediately report any theft of their official mobile devices through the IT Support Desk.

Mobile usage is allowed at Safex Group.

Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password. Employees agree to never disclose their passwords to anyone.

5.7 Email Usage

Users shall ensure that the corporate email facility is used for official purposes only.

Users shall be responsible for the content of email originating from their official email ID.

Users shall refrain from using their official email ID for personal communications.

Users shall not allow others to use their official email ID for any kind of email communication.

Users shall refrain from using others' official email ID for any kind of email communication.

Users are prohibited from sending, receiving, or forwarding following categories of emails using official email facility:

Emails containing defamatory, offensive, racist, or obscene remarks.

Emails that contain viruses or worms.

Chain mails like mails forwarded from a chain of people usually containing hoaxes, jokes, music, movies, and others.

Emails containing any document, software, or other information protected by copyright, privacy, or disclosure regulation.

Users shall exercise caution in providing their official email account to external websites such as discussion boards/ mailing list etc.

Users shall be aware that they are provided with a fixed amount of mailbox space for various official email communications.

Users shall ensure that any email communications are within the fixed size for transmission and any oversized communication shall be made through other appropriate channels as authorised by the IT Department.

Users shall use the official email client i.e., Official Mailing service for all kinds of official email communications.

Users shall be aware that they are responsible for management of any local copy of the mailbox that they are storing in their laptop or desktop.

User shall password protect the local copy of mailbox with a strong password the password should be as per the password policy.

Users shall ensure that email communication containing sensitive information is protected during transmission using appropriate mechanisms as authorised by the IT Department.

Users shall promptly report any kind of security incidents related to the e-mail system to the IT Support Desk.

Users shall be aware that Safex Group reserves the right to monitor email messages and may intercept or disclose or assist in intercepting or disclosing email communications to ensure that email usage is as per this policy. Safex Group may use the intercepted email as evidence to prosecute the user if required.

Users shall be held responsible for any misuse of email communication originating from their account. In the event of misuse, the user's email account shall be terminated, and adequate disciplinary actions may be taken.

5.8 Internet Usage

Access to the internet is based on project and business requirements only.

Users shall ensure that the corporate internet facility is used strictly for Safex Group official purposes only.

Users shall refrain from establishing unauthorised means of accessing internet using Safex Group client devices through personal modems, mobile cards, unauthorised wireless access points etc.

Users shall ensure that they follow appropriate authentication mechanisms to access the internet through the corporate internet facility.

Users shall ensure that they do not access the corporate internet facility with credentials of another user.

Users shall ensure that they do not allow another user to access the corporate internet facility with his/her credential.

Users shall not use corporate internet facilities to access illegal or unethical websites propagating information on gambling, obscene material, violence, weapons, drugs, racism, hate and other similar explicit contents.

Users shall not share official information with external websites unless otherwise authorised by the management.

Users shall not use the internet to download and distribute malicious software in the corporate network of Safex Group.

Users shall promptly report any kind of security incidents related to the internet through the Service Desk.

Users shall be held responsible for any misuse of Internet access originating from their account.

5.9 Printer Usage

Access to the printer is provided based on project/business requirements only.

Users should use Safex Group printing facilities for official purposes only.

Only the necessary pages in the document are to be printed and double-sided printing should be done wherever possible, unless otherwise the business needs printing on a single side.

A networked printer should be made available to staff within close proximity to their work area.

A photocopier should be used in preference to printers when producing a large number of copies.

Confidential information which is printed should be collected from the printer immediately.

When applicable the user shall ensure the information classification is included in the header or footer of the print page.

The users shall ensure any uncollected printed papers shall be shredded securely, if unclaimed at the end of day.

The usage of printers by individuals shall be monitored by the IT department.

Only authorised users shall print confidential documents or information on need basis.

Using appropriate controls, the IT department shall restrict users from printing certain secret or confidential information.

5.10 Document & Record Usage

Users shall handle all documents or records, created both in paper and electronic format, in a secured manner as per their classification levels.

Users shall refrain from accessing or attempting to access any information that is not directly related to fulfilling their job responsibilities.

Users shall ensure that all kinds of documents and records, both in physical and electronic format, are transferred in a secure manner with sufficient security controls.

Users shall ensure that any changes to documents and records are carried out by the authorised person (s) after sufficient review.

Users shall ensure that all documents and records are distributed in a secure manner to avoid any unauthorised accesses.

Users shall ensure that all kinds of official paper documents are shredded before disposal

Users shall ensure that the storage devices namely USB's, hard disks, CDs, DVDs are formatted or degaussed before disposal.

5.11 Removable Media Usage

This policy shall be applicable to the following.

1. Computers
2. Hard disks
3. USB Tokens/Pen drives

A request to be sent by the personnel who would want movement of the above identified materials as following:

Input	Manager	System Administrator	IT Manager	IT Head
Request to be sent to	Yes	Yes	Yes	Yes

Installation of the above listed media shall require approval as identified.

The personnel shall seek approval, before copying data to any kind of media or enabling the ports for the zip drives or USB tokens from the management using the request form.

5.12 Unacceptable use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities:

Under no circumstances is an employee authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Safex Group information systems. The lists below provide a framework for activities that fall into the category of unacceptable use.

5.12.1 System and network activities

The following activities are strictly prohibited, with no exceptions:

Unauthorised copying of copyrighted material, downloading/ distributing/ storage of pornography, MP3, audio, video, games etc. is not acceptable. Downloading/installing/using freeware/shareware or any software tools which are non-business in nature/not approved by the business.

Revealing your credentials to others or allowing use of your credentials by others.

Sharing company/ official information, employee personal information or client provided information with unauthorised personnel within or outside of the company.

Using a Safex Group information system to actively engage in procuring or transmitting material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, defamatory, or otherwise inappropriate or unlawful.

Tampering, disengaging or otherwise circumventing information systems security controls.

Making fraudulent offers of products, items, or services originating from any Safex Group's account.

Affecting security breaches or disruptions of network communication.

Port scanning or security scanning.

Circumventing user authentication or security of any host, network, or account.

Using any program/ script/ command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the Internet/ Intranet/ Extranet.

Access - Users are required to be aware of locking and access restriction mechanisms. Users are responsible to secure and maintain integrity of account(s), passwords or similar information or devices used for identification and authorization purposes. Users shall not share any of the identification and authorization methods with others.

5.12.2 Photography

Photography is in general forbidden within all Safex Group facilities except for passage, cafeteria, and the courtyard. Inadvertent loss of information can happen through photos of screens or documents with data on them.

Photos of structure and layout of Safex Group controlled workspaces, whether office, admin or security facilities is Safex Group Confidential information and the standard rules of dealing with such information will apply.

Valid business approval is needed for photography to be permitted within premises for business reasons. In such a case user must ensure:

1. Photos cannot cover any computer screen/ whiteboard/ projection screen with Safex Group data and/ or client data on it.
2. Camera must be registered with security.
3. All photos taken in prohibited areas need to be deleted from camera and need to be held and reviewed by business approver. The approver must ensure any photography must comply with all provisions in this Policy.

6. Work From Home Guidelines

It is imperative for every employee that any remote access connection used to conduct Safex Group business be utilised appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

Employees will use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with Safex Group's password guidelines. Employees agree to never disclose their passwords to anyone.

All remote computer equipment and devices used for business interests, whether personal or company-owned, must display reasonable physical security measures. Computers need to have company approved antivirus software deemed necessary by Safex Group's IT department.

Any remote connection that is configured to access Safex Group's resources must adhere to the authentication requirements of Safex Group's IT department. In addition, all hardware security configurations (personal or company- owned) must be approved by Safex Group's IT department.

Employees will make no modifications of any kind to the remote access connection without prior approval of Safex Group's IT department. This includes, but is not limited to, non- standard hardware or security configurations, etc.

Employees with remote access privileges must ensure that their computers are not connected to any other network while connected to Safex Group's network via remote access, with the obvious exception of Internet connectivity.

Remote access privileges must never use non-company e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct Safex Group's business.

Remote access facility shall not be misused, and the user shall be held responsible for any misuse traced back to his/her login credentials. No employee is to use Internet access through company networks via remote connection for the purpose of illegal transactions, harassment, competitor interests, or obscene behaviour, in accordance with other existing employee policies.

If a personally-or company-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorised user will be responsible for notifying their manager and Safex Group's IT department immediately.

The remote access user also agrees to immediately report to their manager and Safex Group's IT department any incident or suspected incidents of unauthorised access and/or disclosure of company resources, databases, networks, etc.

All user activities with respect to remote access shall be logged and monitored for the remote access user and he/she also agrees to and accepts that his or her access and/or connection to Safex Group's networks may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity.

7. Enforcement

7.1 Policy violations

Violation of the Policy will result in corrective action from the management. Disciplinary action will be initiated consistent with the severity of the incident as determined by the investigation, and may include, but not limited to:

Loss of access privileges to information assets

Termination of employment or contract

Other actions deemed appropriate by Management

Violation of the policy shall be reported to the **IT Head**

8. Document References

Document/ Form No.	Title
Tracker	Asset Stolen Tracker
Tracker	Asset Disposal Tracker
Tracker	Warranty Tracker
Tracker	AMC Tracker
Tracker	Data Destruction Tracker

Suresh
01/04/23