Safex Group

Safex
Caring for you to grow

Indo Swiss
Smith & Smith
HIM bio agro
Agcare

BCS Best Crop Science
Shogun Lifesciences Pvt. Ltd
Shogun Organics Limited

Information Security Policy

Suresh
01/04/23

Safex Group.

Information Security Policy

1. Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Information Security Policy
2.	Document Code	ITISP01
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	29-03-2023
2			
3			

Suresh
01/04/23

2. Policy Statement

The use of **Safex Group.** (hereinafter referred as "**Safex Group**" or the "Company") electronic systems, including computers, fax machines, and all forms of internet access, is for Company's business and for authorized purposes only. Brief and occasional personal use of the electronic mail system or the internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time *(lunch or other breaks)*, and does not result in expense or harm to the Company or otherwise violate this policy.

The Information Security Policy ('ISP') applies to all assets *(i.e., physical assets, paper assets, people assets, information assets, site as an asset, software assets and services as an asset)* at **Safex Group**. The ISP applies to all IT technologies and services *(i.e., storage, application services etc.)* that are delivered as an enabler to support Safex Group's business delivery.

As part of the policy the following departments are covered:

- Information Technology ('IT')
- Human Resource/Administration
- Finance
- Accounts
- Sales/Marketing
- Supply Chain/Purchase/Taxation

The policy states:

- Security of assets of Safex Group Is of paramount importance. Confidentiality, integrity, and availability of the assets shall be maintained at all times through controls that are commensurate to the criticality of the asset, so as to protect the assets from all types of threats, whether internal or external, deliberate, or accidental.
- That all forms of information *(electronic/ print)* on any medium will be classified and protected as per information security requirements.
- Information Technology (IT) department shall be responsible for conducting security awareness training for all staff.
- Compliance to all business, legal or regulatory, contractual, and other applicable requirements and obligations will be ensured.
- That the approved ISP document shall be communicated or made available to all employees and external parties having access to **Safex** Group's information or information processing facilities *(as appropriate)*.
- Background check shall be done by HR for all staff during recruitment as part of the screening process.
- All employees shall sign a confidentiality or non-disclosure agreement at the time of joining. This shall be incorporated as part of terms and conditions of employment.
- Human Resources (HR) shall notify the end of service or suspension/termination of an employee to the Information Technology (IT) department.

- The IT Department is responsible for revoking all the logical access rights (email id, simplify id (not applicable to factory workers) and SAP id) of leaving employees and return of all organizational assets possessed by the employee.
- Any changes to the ISP shall be approved initially by the AVP (IT) and finally by the Group Director .
- ISP shall be approved by **Safex Group** management, published and communicated to all concerned.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the Company's business; distract, intimidate, or harass co-workers or third parties; or disrupt the workplace.

Use of Company computers, networks, and internet access is a privilege granted by Management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial email ("spam") that is unrelated to legitimate Company purposes;
- Engaging in private or personal business activities;
- Accessing networks, servers, drives, folders, or files to which you have not been granted access or authorization from someone with the right to make such a grant;
- Making unauthorized copies of Company files or other Company data;
- Destroying, deleting, erasing, or concealing Company files or other Company data, or otherwise making such files or data unavailable or inaccessible to the Company or to other authorized users of Company systems;
- Misrepresenting oneself or the Company;
- Violating the laws and regulations of India or any other nation or any state, city, or other local jurisdiction in any way;
- Engaging in unlawful or malicious activities.
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Company's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems;
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Defeating or attempting to defeat security restrictions on Company systems and applications.

Using Company electronic systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates the Company anti-harassment policies and subjects the responsible employee to disciplinary action. The Company's electronic mail system, internet access, and computer systems must not be used to harm others or to violate Indian laws and regulations or any other nation or any state, city, or other local jurisdiction in any way. Use of Company resources for illegal activity can lead to disciplinary action, up to and including dismissal.

If you violate these policies, you could be subject to disciplinary action, up to and including dismissal.

Approval for exceptions or deviations from the ISP, wherever warranted, will be provided only after an appropriate assessment of the risks arising out of providing the exception. This assessment will be conducted by the IT team. Exceptions will not be universal but will be agreed on a case-by-case basis, upon official request made by the asset owner. These may arise, for example, because of local circumstances, conditions or legal reasons existing at any point of time. Exceptions to the ISP may have to be allowed at the time of implementation of policies and guidelines or at the time of making any updates to this document or after implementation *(ad-hoc).*

3. Segregation of duties

Segregation of duties is required so that no single user has the ability to subvert any security controls of the information systems that would negatively impact the business operations. The functional heads are required to ensure that no employee in their function is responsible for multiple duties such that it could lead to the circumvention of the existing security control*(s).*

- Segregation of duties shall be ensured across **Safex** Group's information systems, but not limited to the following departments:
  a. Business system use
  b. Computer/ IT systems operations and administration
  c. System development and maintenance
  d. Security administration
- If it is difficult to segregate duties, controls such as monitoring of activities, audit trails, management supervision and independent reviews shall be implemented to mitigate the risks.
- The duties and areas of responsibilities of employees shall be segregated and records of the same shall be maintained to reduce the opportunities for unauthorized or unintentional modification or misuse of information assets. In cases where segregation of duties is not possible, approval of the department head shall be obtained prior to allocating responsibilities to the employee. Also, appropriate compensatory controls such as monitoring of activities, management supervision and independent reviews shall be implemented.

4. Mobile devices and teleworking

A formal process shall be developed and established to safeguard and prevent leakage of information through mobile devices such as laptops and other mobile devices owned and managed by Safex Group IT department. It shall include, but not be limited to the following:

a. Latest virus definitions shall be regularly updated on the mobile devices and systems *(laptops/ desktops)*;

b. Access to Safex Group network shall be protected via the user authentication *(e.g., user ID and password)* and inactive session timeout controls, if applicable;

c. It shall be the employee's responsibility to ensure every effort at their disposal is taken to protect Safex Group's mobile devices and the information stored in these devices.

d. Awareness sessions *(if needed)* shall be conducted for the employees, using mobile computing, to increase their awareness on the additional risks resulting from this way of working and precaution that needs to be taken while using the device.

- Mobile device policy

  Security measures shall be adopted to manage the risks introduced by using mobile devices.

  a. Bring Your Own Device ('BYOD') – Employees including third-party, contractual and interns are not allowed to bring personal computing devices such as, but not limited to, personal laptops, tablets *(iPad, surface etc.)* unless an exception approval has been given by AVP (IT). In case such a device is brought to office inadvertently, the employee will declare and deposit the same at the reception. The Company will not be liable for any damage whatsoever to said property and shall endeavor to store the same on a best effort basis.

  b. Employees are required to take special care of the mobile computing resources such as, but not limited to, laptops, mobile phones, handheld computing devices to prevent any compromise and/ or destruction of business information. Employees would be liable for all loss/ unauthorized access/ unauthorized disclosure or sharing of information/ data as a result of usage of employee personal devices.

c. Latest virus definitions shall be regularly updated on laptops to minimize the risk of virus attacks and corruption/ theft of information stored on these devices;
d. Firewalls should be installed with appropriate policies configured on them;
e. Third-party staff shall not be allowed to connect their computing devices to Safex Group' network unless authorized by the functional heads; &
f. Personal data shall not be downloaded on any mobile device. Any personal data stored on mobile devices shall be deleted.

- Teleworking

Teleworking requests shall be handled in accordance with the approved procedures. Adequate teleworking security measures shall be established and implemented. At a minimum, the following controls shall be implemented:

a. Establishing a secure communication channel between the teleworkers and the Safex Group network;
b. Revocation of authority, access rights and return of equipment when the teleworking activity ceases or the employee exits from Safex Group; &
c. Employees working from home shall ensure adequate security to protect Safex Group' equipment and data.

5. Email Usage

- **User Account**

Upon joining, your information is passed to IT by the HR department. IT generates a unique email ID, and this email ID and associated information is conveyed to HR, Admin and Payroll and IT helpdesk for configuring the appropriate access in respective systems and allocate IT assets. After completing the configuration and preparation of allocated IT assets, the IT intimates the employee's email address, temporary password, and hands over the assets to the user.

- **User ID and Password**

Your User ID identifies you to Safex Group email systems and your password authenticates you. Password security can be expressed by five simple rules:

a. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Safex Group Information. Keep it private. If you need to share computer resident data, use electronic mail, public direAVP (IT)ries on local area network servers, and other mechanisms.
b. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices *(phone, tablet)* without encryption. Keep it secret. If you must write it down, store the paper in a secure place, and destroy it properly when no longer needed.
c. Make sure it cannot be guessed by anyone or program in a reasonable time.
d. If you suspect that your password has been compromised, you must report the incident to IT to change your password and check the security settings.
e. Ensure that you change your password at regular intervals. The recommended change interval is every two months.
f. Following password standards shall be adhered with:

For Laptops

S.No.	Particulars	Requirement
1.	Minimum password length	8
2.	Standard	Alphanumeric
3.	Minimum number of characters which differ between old and new password	3
4.	Character set use for passwords	1
5.	Login/ password expiration time	90 days
6.	New Password not set at least for	Last 3 passwords

For SAP

Parameters	Current Value	Value Description	Description
login/disable_cpic	1	Refuses	[0: Allow] [1: Refuses inbound connections of type CPIC. Inbound connections of type RFC remain unaffected.]
login/disable_multi_gui_login	1	Block	[0: Allow] [1: The system blocks multiple dialog logons in the same client and under the same user name.]
login/disable_password_logon	0	Possible	[0: Password logon is possible] [1: Password logon is only possible for users in the group specified in the parameter login/password_logon_usergroup.] [2: Password logon is not possible in general]
login/failed_user_auto_unlock	0	Lock	[0: Locks due to incorrect logon attempts remain valid for an unlimited period] [1: Unlock after unspecified period]
login/fails_to_session_end	3	Enabled	[3: Session locked after 3 invalid attempts]
login/fails_to_user_lock	5	Enabled	[5: User locked after 5 invalid attempts]
login/min_password_digits	1	Enabled	[0: No numeric digit required] [1: At least one numeric digit required]
login/min_password_letters	1	Enabled	[0: No characters required] [1: At least one character required]
login/min_password_lng	10	Enabled	[0: No length required] [10: Min. length required]

login/min_password_ lowercase	1	Enabled	[0: No character required in lower case] [1: At least one character required in lower case]
login/min_password_ specials	0	Disabled	[0: No special character in required] [1: At least one special character in required]
login/min_password_ uppercase	1	Enabled	[0: No character required in upper case] [1: At least one character required in upper case]
login/multi_login_users	0	Locked	[0: Multi login locked] [1: Multi login required]
login/no_automatic_ user_sap*	1	Activated	[0: emergency user (sap*) disable] [1: emergency user (sap*) user activated]
login/password_change_ for_SSO	1	Enabled	[0: Requirement to change password is ignored (backward compatible)] [1:Password change dialog only (enter: old and new passwords)]
login/password_compliance _to_current_policy	1	Enabled	[0: No Check] [1: During the password check, the system checks whether the current password fulfills the current password rules. If this is not the case, it forces a password change.]
login/password_expiration _time	90	Enabled	[0 - 1000: Defines the validity period of password in days.]
login/password_history _size	15	Enabled	[0: No history of password stored] [15: Fifteen history of password stored]
login/password_max_ idle_initial	7	Enabled	[0: No idle initial] [7: 7 days idle initial]
login/system_client	600	Enabled	[600: Default client for production]

For Email

Parameters	**Current Value**	**Value Description**	**Description**
Strength	Strong Password	Enabled	Passwords should be a combination of letters, numbers, and symbols.
Minimum length of password	8	Enabled	[0: No length required] [8: Min. length required]
Maximum length of password	20	Enabled	[0: No length required] [20: Max. length required]
Strength and length enforcement	Enabled	Enabled	Changes to length and strength requirements are applied the next time an affected user changes their

			password. To apply changes immediately, start enforcement the next time a user signs in.
Password expiry time	90	Enabled	[0 - 1000: Defines the validity period of password in days.]
Session expiry time (Enterprise Lic)	12	Enabled	[0 - 100: Defines the validity period of a session on the browser in hours.]
Session expiry time (Business Starter Lic)	14	Enabled	[0 - 100: Defines the validity period of a session on the browser in days.]

- General Email Guidelines

a. **Business Email Use:** Safex Group Recognizes that email is a key communication tool. We encourage our Employees to use email in an appropriate manner to communicate within and outside the organization.

b. **Personal Use of Email:** The Company also recognizes that email is an important tool in everyone's daily lives. As such, it allows you to use your Company email account for personal reasons, with the following stipulations:

✓ Personal email use should be of a reasonable level.

✓ All rules described in this policy apply equally to personal email use. For instance, inappropriate content is always inappropriate, no matter whether it is being sent or received for business or personal reasons.

c. You are not permitted to "blanket forward" *(the automatic forwarding of every email received)* your **Safex Group Email** messages, or forward confidential messages to a personal account obtained through a third-party internet service provider *(for example, Hotmail, AOL, Yahoo, Gmail etc.)*.

- **Email Security**

Used inappropriately, email can be a source of security problems for the Company. Users of the Company email system must not:

a. Open email attachments from unknown sources, in case they contain a virus, Trojan, spyware or other malware.

b. Disable security or email scanning software. These tools are essential to protect the business from security problems.

c. Send confidential Company data via email. The IT department can advise on appropriate tools to use instead.

- **Inappropriate Email Content and Use**

The Company email system must not be used to send or store inappropriate content or materials. It is important that you understand that viewing or distributing inappropriate content via email is not acceptable under any circumstances.

Users must not:

a. Write or send emails that might be defamatory or incur liability for the Company.

b. Create or distribute any inappropriate content or material via email.

Inappropriate content includes pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism, or materials relating to cults, gambling, and illegal drugs.

This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

a. Use email for any illegal or criminal activities.

b. Send offensive or harassing emails to others.

c. Send messages or material that could damage Safex Group' image or reputation.

Any user who receives an email they consider to be inappropriate should report this to their Reporting Manager or the HR department.

- **Copyright**

  Safex Grouprespects and operates within Copyright laws. Users may not use Company email to share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.

  You must not use the Company's email system to perform any tasks that may involve breach of copyright law.

- Users should keep in mind that the copyright on letters, files and other documents attached to emails may be owned by the email sender, or by a third party. Forwarding such emails on to other people may breach this copyright. Such kind of breach may result in disciplinary measures being taken.

- **Contracts and Liability**

  You must be careful about making commitments or agreeing via email. Make sure that you are authorized to make a particular commitment before sending any confirmation via email.

  An email message may form a legally binding contract between Safex Group And the recipient — even if you have not obtained proper authorization within the Company.

- **Monitoring Email Usage**

  Safex Group Email system and software are provided for legitimate business use. Safex Group Therefore reserves the right to monitor your use of email.

  Any such examinations or monitoring will only be carried out by authorized staff. Additionally, all emails sent or received through the Company's email system are part of official Safex Group Records. Safex Groupcan be legally compelled to show that information to law Enforcement Agencies or other parties. Users should always ensure that the business information sent via email is accurate, appropriate, ethical, and legal.

6. Internet Use

Safex Group makes internet access available to you as it is relevant and useful for their jobs.

It is important every person at the Company who uses the internet understands how to use it responsibly, safely, and legally.

Proper Internet Use:

a. Reduces the online security risks faced by Safex Group.
b. Ensures that you do not view inappropriate content at work.
c. Helps the Company satisfy its legal obligations regarding internet use.

- **General Internet Guidelines**

Safex Group recognizes that the internet is an integral part of doing business. It therefore encourages you to use the internet whenever such use supports the Safex Group' goals and objectives.

Personal Internet Use

Safex Group also recognizes that the internet is embedded in everyone's daily lives. As such, it allows you to use the internet for personal reasons, with the following stipulations:

a. Personal internet use should be of a reasonable level.
b. All rules described in this policy apply equally to personal internet use. For instance, inappropriate content is always inappropriate, no matter whether it is being accessed for business or personal reasons.
c. Personal internet use must not affect the internet service available to other people in the Company. For instance, downloading large files could slow access for other employees.

- **Internet Security**

Used unwisely, the internet can be a source of security problems that can-do significant damage to the Company's data and reputation.

a. Users must not knowingly introduce any form of computer virus, trojan, spyware or other malware into the Company.
b. You must not gain access to websites or systems for which they do not have authorization, either within the business or outside it.
c. Company data should only be uploaded to and shared via approved services. The IT department can advise on appropriate tools for sending and sharing large amounts of data.
d. You must not steal, use, or disclose someone else's login or password without authorization.

- **Inappropriate Content and Uses**

There are many sources of inappropriate content and materials available online. It is important for you to understand that viewing or distributing inappropriate content is not acceptable under any circumstances. You must not:

a. Take part in any activities on the internet that could bring Safex Group into disrepute.
b. Create or transmit material that might be defamatory or incur liability for Safex Group.
c. View, download, create or distribute any inappropriate content or material.

- **Copyright**

Safex Grouprespects and operates within copyright laws. You must not use the internet to:

a. Publish or share any copyrighted software, media or materials owned by third parties, unless permitted by that third party.
b. Download illegal copies of music, films, games, or other software, whether via file sharing services or other technologies.

You must not use the Safex Group' equipment, software, or internet connection to perform any tasks which may involve breach of copyright law.

All Safex Grouppolicies and procedures apply to your conduct on the internet, especially, but not exclusively, relating to intellectual property, confidentiality, Company information dissemination, standards of conduct, misuse of Company resources, anti-harassment, and information and data security.

- **Networks**

Local Area Network ("LAN") and Wide Area Network ("WAN" or "Wi-Fi") infrastructure hardware is purchased, installed, and managed by the IT department. Only approved equipment may be attached to the LAN and WAN, and any changes to the networks may only be approved by authorized IT. You are not allowed to use software/ hardware to monitor network or network components or capture packets unless it is approved by the IT Head.

The following activities are strictly prohibited, with no exceptions:

a. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
b. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which you are not an intended recipient or logging into a server or account that you are 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, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
c. Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.
d. Executing any form of network monitoring which will intercept data is not intended for your host unless this activity is a part of your normal job/ duty.
e. Interfering with or denying service to any user other than your host *(for example, denial of service attack).*
f. 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.

7. Social Media Use

At Safex Group, we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends, and co-workers around the world. However, use of social media also presents certain risks and carries certain responsibilities with it. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media.

This policy applies to all associates who work for and with us.

- **Guidelines**

In the rapidly expanding world of electronic communication, social media can mean many things. The term "Social Media" includes all means of communicating or posting information or content of any sort on the internet, including to your own or someone else's web log or blog, journal, or diary, personal website, social networking or affinity website, web bulletin board, or a chat room, whether or not associated or affiliated with Safex Group, as well as any other form of electronic communication.

The same principles and guidelines found in Safex Group' policies apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow associates or otherwise adversely affects members, customers, suppliers, people who work on behalf of Safex Groupor Safex Group' legitimate business interests may result in disciplinary action up to and including termination.

- Know and follow the rules

Carefully read these guidelines and ensure your postings are consistent with Safex Grouppolicies. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated.

- **Be Respectful**

Always be fair and courteous to fellow associates, customers, members, suppliers, or people who work on behalf of Safex Group. Also, keep in mind that you are more likely to resolve work-related complaints by speaking directly with your co-workers or by utilizing our channels of communicating and reporting, if required, than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video, or audio that reasonably could be viewed as malicious, obscene, threatening, or intimidating, that disparage customers, members, associates, or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion etc.

- **Be Honest and Accurate**

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about Safex Group, fellow associates, members, customers, suppliers, people working on behalf of Safex Group, or competitors.

- **Post Only Appropriate and Respectful Content**

a. Maintain the confidentiality of the Safex Group' trade secrets and private or confidential information. Trade secrets may include information regarding the development of systems, processes, products, know-how, and technology. Do not post internal reports, policies, procedures, or other internal business-related confidential communications.
b. Do not create a link from your blog, website, or other social networking site to Safex Group' website without taking prior and appropriate approvals.
c. Express only your personal opinions. Never represent yourself as a spokesperson for Safex Group. If Safex Groupis a subject of the content you are creating, be clear and open about the fact that you are an associate and make it clear that your views do not represent those of Safex Group, fellow associates, members, customers, suppliers, or people working on behalf of Safex Group. If you do publish a blog or post online related to the work you do or subjects associated with Safex Group, make it clear that you are not speaking on behalf of Safex Group. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of Safex Group."

- **Using Social Media at Work**

  Refrain from using social media while on work time or on equipment we provide unless it is work-related as authorized by your manager or consistent with **Safex Group** Policy. Do not use Safex Group' email addresses to register on social networks, blogs, or other online tools utilized for personal use.

8. Anti-Virus Guidelines

The IT department is responsible for the following:

- Anti-virus protection strategy shall be developed and implemented.
- Anti-virus controls shall be established at all the network entry points connecting to the Internet. Users shall not be able to disable the software in their desktops or laptops.
- The Assistant Manager (IT) shall be responsible for monitoring and performing log analysis of the logs generated by the anti-virus application on a monthly basis.
- Anti-virus logs shall be maintained on a regular basis and reviewed on a monthly basis.
- Logs generated by the Antivirus application shall be stored, filtered, correlated, and analyzed.
- Emergency response procedures shall be established to handle break out of virus incidents.

Recommended processes to prevent virus problems:

- Always run the corporate standard, supported anti-virus software available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding it.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/ write access unless there is absolutely a business requirement to do so.
- Always scan a USB media from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If lab testing conflicts with antivirus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

Metrics:

The IT department should prepare a report on the following:

a. Number of systems without Antivirus agent installed.

b. Number of agents not getting updated in a timely manner.

c. Total number of instances of infection.

d. Number of instances of infections not cleaned automatically.

9. Data Protection

- Data includes *(but not limited to)*:
  a. Names of individuals
  b. Postal addresses
  c. Email addresses
  d. Telephone numbers
  e. any other information relating to individuals.

- **Data Protection Risks**

  Data security risks, include:
  a. Breaches of confidentiality. For instance, information being given out inappropriately.
  b. Failing to offer choice. For instance, all individuals should be free to choose how the Company uses data relating to them.
  c. Reputational damage. For instance, the Company could suffer if hackers successfully gained access to sensitive data.

- **Responsibilities**

  Everyone who works for or with **Safex Group** has some responsibility for ensuring data is collected, stored, and handled appropriately.

  Each team that handles Personal Data must ensure that it is handled and processed in line with this policy and data protection principles. They are responsible for:
  a. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  b. Performing regular checks and scans to ensure security hardware and software is functioning properly.
  c. Evaluating any third-party services, the Company is considering using to store or process data. For instance, cloud computing services.

- **General Guidelines**

  a. The only people able to access data covered by this policy should be those who need it for their work.
  b. Data should not be shared informally. When access to confidential information is required, you can request it from their line managers.
  c. **Safex Group** will provide training to you to help you understand your responsibilities when handling data from time to time.
  d. You should keep all data secure, by taking sensible precautions and following the guidelines below.
  e. In particular, strong passwords must be used, and they should never be shared.
  f. Personal data should not be disclosed to unauthorized people, either within **Safex Group** or externally.
  g. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
  h. You should request help from the IT department if they are unsure about any aspect of data protection.

- Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager:

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

a. When not required, the paper or files should be kept in a locked drawer or filing cabinet.
b. You should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.
c. Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts:

a. Data should be protected by strong passwords that are changed regularly and never shared between employees.
b. If data is stored on removable media *(like a CD or DVD or pen drive or hard disk)*, these should be kept locked away securely when not being used.
c. Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
d. Servers containing personal data should be sited in a secure location, away from general office space.
e. Data should be backed up frequently. Those backups should be tested regularly, in line with the Company's standard backup procedures.
f. Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
g. All servers and computers containing data should be protected by approved security software and a firewall.

- **Disclosing Data for Other Reasons**

In certain circumstances, the data is required to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, **Safex Group**will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the Company's legal advisers where necessary.

- **Providing Information**

Safex Group aims to ensure that individuals are aware that their data is being processed, and that they understand:

a. How the data is being used
b. How to exercise their rights

To these ends, the Company has a privacy statement, setting out how data relating to individuals is used by the Company.

[This is available on request. A version of this statement is also available on the Company's website]

10. Asset Management - IT Asset/ Laptop/ Accessories Uses

This section on asset management specifies the importance of information assets including identification of the asset owner, asset classification and determining confidentiality, integrity, and availability ratings of the assets.

It establishes the requirement of controls that need to be implemented for protecting information assets. **Safex Group** shall ensure that all assets *(physical, informational, paper, people, services, site, and software)* shall be managed and protected. **Safex Group** shall ensure proven, reliable, and approved hardware/ software assets are deployed and maintained to meet security requirements and to reduce the risk of information security being compromised by weakness in hardware/ software due to poor asset management.

- **Inventory of Assets**

All **Safex Group**' assets are listed in the IT asset register and shall contain the following information as a minimum:

a. Type and location of the asset; &
b. Asset owner, custodian, and user

- **Ownership of Assets**

The asset owner shall be responsible for the appropriate maintenance and protection of the information. The asset owner may delegate the responsibility of the maintenance and protection of the asset to an individual/ department referred to as "Asset Custodian".

- **Laptop and Consumables Accessories**

Issuance of Laptop

At the time of issuance of the laptop, you need to make sure that there are no damages in the issued assets. If there is any, the same should be immediately notified to the IT department. Once the asset has been handed over to you, it becomes your responsibility to keep the asset in good condition. You will be personally responsible for any damage in the laptop in his possession.

Responsibility on Laptops:

a. Do not physically drop or bump your laptop.
b. Do not place heavy objects on your laptop.
c. Do not spill or allow liquid to be spilled onto your laptop.
d. Do not disassemble your laptop.
e. Do not place your laptop near any equipment which generates a strong magnetic field.

Extend your Laptop Computer's Battery Life by Doing the Following:

a. Remove a PC card if it is not in use.
b. Decrease the LCD brightness.
c. Drain out your battery completely and recharge it again whenever possible.

Accessories

a. All IT accessories are procured and stored by the IT department. You need to submit a request via email. The consumables shall be issued post request is approved *(as per applicable process)* and if the accessories are in stock. The IT department shall put in their best efforts to maintain the consumables stock.

b. If there is any request due to loss or damage to the accessory, the cost of replacement will be borne by the user. Upon paying the cost of replacement, the same will be provided to the user or at the discretion of management.

c. Since there is no end of life or insurance for accessories, in case of loss/ damage, the total cost of the accessories will be borne by the end users.

- **IT Assets**

Hardware

The detailed inventory of all Safex Group' IT equipment is maintained by Safex Group' IT department. All IT related equipment may only be purchased through IT, following the process in place. Any loss/ damage to the equipment must be reported immediately to the IT department. Any transfer of equipment *(between two individuals as well as locations)* must be initiated only by the IT department.

In case of physical/ liquidity damage to the equipment caused by you, the situation shall be evaluated on a case-to-case basis and you might be required to pay for the damage so caused or the repair cost incurred for the damage so caused.

Software Installation

a. You must not install software on Safex Group' computing devices operated within the Safex Group network.

b. Software requests must first be approved by your manager and then be made to the IT department or service desk in writing or via email.

c. The IT department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

- **Personal Electronic Equipment Use**

Safex Group prohibits the use in the workplace of any type of camera phone, cell phone camera, digital camera, video camera, or other form of recording device to record the image or other personal information of another person or the financial or any other information of Safex Group, if such use would constitute a violation of a statute that protects the person's right to be free from harassment or from invasion of the person's right to privacy or violation of Safex Group policy on data security, as the case may be.

To minimize the risk of unauthorized copying of confidential Company business records and proprietary information that is not available to the general public, any employee connecting a personal computing device, data storage device, or image-recording device to Safex Group networks or information systems thereby gives permission to Safex Group to inspect the personal computer, data storage device, or image-recording device at any time with personnel and/or electronic resources of the Safex Group' choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the data-storage device in question in order to ensure that confidential Company business records and proprietary information have not been taken without authorization. Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not connect them to Safex Group computers or networks.

- **Replacement**

  If you have a laptop which is older than three years, you are entitled to replace your laptop based on your department of the Company.

- **Repair and Damage**

  If you have any system issues, the same should be communicated to the IT department.

  While assessing the nature of the complaint, the IT department shall assess whether the damage is on account of physical damage or otherwise. In case of physical damage, the IT department shall assess the cost of such loss and communicate the same to the Finance department and you. In such cases 100% of the cost of damage shall be recovered from you or at the discretion of management.

- **Department Transfer/ Internal Job Posting**

  In case of a change of your work department, you are not automatically entitled to change your laptop. However, if the situation warrants such replacement, you should get approval from your reporting Manager & Chief Finance Officer ('CFO').

- **Lost and Stolen Laptop**

  If your laptop is lost, then you need to immediately contact the IT/ Finance department upon becoming aware of such loss. Further, you need to submit the following documents without any delay:

  a. First-hand Information Report ('FIR')
  b. Please ensure that "missing" is not mentioned in the FIR. The insurance companies interpret "missing" differently from theft and treat that as negligence.

  In case of loss of laptop on account of car theft, please ensure to mention "car was locked" to avoid any negligence angle.

  a. Statement explaining the circumstances leading to the loss.
  b. Related proof supporting the above statement. E.g., Laptop stolen while traveling, then ticket/ boarding pass will be required.
  c. Invoice of any repair done subsequently, if applicable. E.g., Laptop stolen from car by breaking window glass of window.
  d. Final investigation report or non-traceable report from Police.
  e. Claim form – To be filled by the local IT or Finance department in consultation with you.
  f. Laptop Invoice – To be provided by the Finance department.
  g. Proforma invoice of similar make and model - To be provided by the Finance department.
  h. In case, any further documents are required then the same shall be informed.

- **Return of Equipment**

  While leaving the organization, you shall be required to get the IT clearance done by handover of the hardware equipment or software that you possess or else, full, and final settlement of dues shall not be cleared by the Accounts department. The IT department shall approve clearance requests only when all the IT equipment would have been returned to the IT department.

If the IT department identifies that an asset is damaged, you shall remain responsible for the repair/ replacement of the asset/ equipment and the amount will be deducted from your full and final settlement.

11. Physical and Environmental Safety

Safex Group shall provide adequate protection to its information systems and facilities against unauthorized physical access and environmental threats. This section defines appropriate security controls required to protect the information assets and information processing facilities of **Safex Group** from physical and environmental threats.

- **Physical Security Perimeter**
  Appropriate security controls shall be designed and implemented to prevent unauthorized physical access, damage, and modification to **Safex Group'** information processing facility.

  The entry to the **Safex Group** premises shall be controlled by adequate access control mechanisms and guarded by security personnel. The premises entry exit points and especially the critical areas shall be monitored by CCTV cameras at all times.

- **Physical Entry Control**
  All **Safex Group** offices/ premises shall implement physical security controls but not limited to:
  a. Access to restricted area shall be controlled and monitored;
  b. The access shall also be deactivated immediately when the notification is received from any business functions in case of any security breaches;
  c. Security guards shall be stationed at the main entrance to protect against unauthorized access to the premises. The guard shall be on duty 24*7. Doors requiring electronic access controls will be installed at the entrance to each floor;
  d. Visitors shall be asked to declare their assets at the entrance. They shall deposit the restricted assets at the entrance and the same shall be recorded in a register;
  e. Employees shall not permit unknown or unauthorized persons to pass through doors requiring authorization, at the same time when they pass through these entrances; &
  f. The physical security of the **Safex Group** premises shall be reviewed on a regular basis.

- **Securing Offices, Rooms and Facilities**
  a. Depending on the sensitivity of information handled within, the physical security for offices, rooms and facilities shall be designed and applied; &
  b. Access to server rooms or network rooms shall be restricted to authorized **Safex Group** employees only.

- **Protecting Against External and Environmental Threats**
  The Information processing facilities shall be fitted with appropriate fire fighting devices *(i.e., smoke deterrent AVP (IT)rs, fire extinguishers, sprinklers etc.)* in order to detect the fire at the incipient stage, arrest the fire spread and to avoid damage to the resources of **Safex Group.**

  Safex Group shall actively take part in all safety drills like fire and earthquake evacuation drills as and when conducted by the building management team.

- **Working in Secure Areas**
  a. All third-party employees/ vendors shall be accompanied by at least one person from the IT department/ Administration department during their visit to restricted areas *(i.e., the areas where critical information systems or equipment are located is defined as restricted areas. They include but are not limited to server room, network room etc.)* All such visits shall only be for business purposes and will be approved by the respective functional head;
  b. All critical servers and communications equipment shall be located in a restricted area and protected with adequate access control mechanisms;
  c. **Safex Group** will implement adequate controls to protect the areas hosting sensitive information processing equipment from heat, dust, water leakage;
  d. Classified business information, including personal data shall not be left unattended openly or displayed on the screen. Adequate level of awareness shall be made through various awareness programs to **Safex Group**staff on acceptable information systems usage and compliance of physical security measures. All employees shall ensure that their computer screens are locked whenever they leave their desks;
  e. Eating & drinking shall be prohibited in the server room and working areas; &
  f. USB, data card, laptops, mass storage devices and cameras shall be strictly prohibited inside the server/ network room.

- **Delivery and Loading Areas**
  a. It shall be ensured that all areas, where loading and unloading of items are done, are monitored, and equipped with the appropriate physical security controls during these activities; &
  b. Mails/ courier shall be delivered to the security desk. Courier personnel shall not be allowed to enter **Safex Group**' premises unless authorized.

- **Supporting Utilities**
  All equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. All supporting utilities shall be monitored for their availability and maintained as per vendor guidelines.
  a. Uninterrupted electrical power supply ('UPS') and support utilities services, for e.g., air conditioning, heating and ventilation, water supply, sewage are available during all business hours;
  b. UPS systems, generators, fire suppression systems and humidity control systems are installed to support controlled shutdown or continued functioning of equipment supporting critical business operations;
  c. There is liaising in place with appropriate authorities for utilities, emergency services, health and also with safety departments; &
  d. A review of preventive maintenance is conducted by the authorized personnel of the Administration department.

- **Cabling Security**
  Appropriate controls shall be designed and implemented to protect power and network cables carrying data or supporting information services, from unauthorized interception or damage. It shall be ensured that:
  a. Adequate protection is applied to protect power and telecommunications cabling carrying data or supporting information services from interception or damage;
  b. Cables connecting computing equipment and other support equipment shall be neatly organized;
  c. All electrical wiring and LAN cabling shall be structured / concealed cabling;
  d. Circuit breakers of appropriate capacity shall be installed to protect the hardware against overload or short circuit; &

e. Power cables are segregated from communication cables to prevent interference.

- **Equipment Maintenance**
  a. All equipment shall be properly maintained to ensure their continued availability and integrity for proper uninterrupted business activities. Annual Maintenance Contracts using OEM approved vendors shall be used;
  b. IT department shall ensure that preventive maintenance for all IT devices is carried out at regular intervals for continuous availability of these systems;
  c. Maintenance of equipment shall be carried out as per the manufacturer's instructions and specifications;
  d. Routine maintenance and repair shall be carried out by authorized maintenance personnel only;
  e. The equipment maintenance requirement imposed by insurance policies should be complied with; &
  f. All necessary records required to track maintenance history of equipment shall be maintained.

- **Secure Disposal or Reuse of Equipment**
  a. All information/ data and licensed software shall be removed or securely over-written prior to the disposal of any equipment containing storage media;
  b. Destruction/ disposal of media shall be done in accordance with documented methods/ procedures;
  c. The procedure for secure disposal of media shall apply to all equipment owned by **Safex Group**; &
  d. Before sending any equipment outside **Safex Group** premises for repair, it shall be sanitized to ensure that it does not contain any sensitive data.

12. Operations security

Safex Groupshall ensure effective and secure operation of its information systems and computing devices. Appropriate controls shall be implemented to protect the information contained in and/ or processes by these information systems and computing devices.

This section defines the controls that shall be implemented to prevent unauthorized access, misuse or failure of the information systems and processing facilities. Confidentiality, integrity, and availability of information processed by or stored in the information systems shall be maintained.

- **Operational Procedures and Responsibilities**
  a. Procedures shall be developed, documented, and approved when a new information system or service is introduced. The procedure shall include the roles and responsibilities, the necessary activities to be carried out for the operation and maintenance of the system or service and actions to be taken in the event of a failure;
  b. Proper physical and environmental protection shall be established when media or device containing sensitive information is sent by courier or other means;
  c. The procedure shall be designed and developed to ensure the confidentiality, integrity and availability of the specific platform or application. The procedures shall include, but not limited to, the following:
    - ✓ Any automated or scheduled processes that are running on the information systems;
    - ✓ Day-to-day operational tasks that need to be performed by the operator;
    - ✓ Actions to be performed when an error or an exception condition occurs, including the listed contact details of people that may be required to assist or that may be dependent on that service; &
    - ✓ Any maintenance/ support agreements/ SLAs with the details of the contact names, commencement, and termination dates of agreements.

d. All functional heads shall ensure that the procedures are updated at periodic intervals or at the time of any system change*(s)*. The updated procedures shall be duly approved and released by the respective functional heads;

e. The procedure shall facilitate building or rebuilding of the information system. There shall be adequate details in the Procedure to ensure compliance*(s)* to the baseline security and operational requirements when the build of system/ application is completed; &

f. Security baselines shall be developed, reviewed, approved, and implemented to protect **Safex Group'** information systems. Responsibilities for security baselines shall be as follows:

✓ Developing – Pravesh Chaudhary

✓ Approving and reviewing – Group Director

✓ Implementing – Abhinav Thakur

- **Separation of Development Environment, Testing and Operational Environment**

a. The production environment shall be logically or physically separated from the development and test environments;

b. The change management procedure shall be followed for implementing any change to the production environment;

c. Physical access to the production environment shall be restricted to authorized personnel; &

d. All test data, temporary accounts and temporary passwords shall be removed from the systems prior to deploying them into the production environment as per the system hardening process.

13. **Backup**

Information backup and restoration shall be performed to ensure the integrity and availability of business information. Backup copies of information, software and system images shall be taken and tested regularly to prevent any loss of data causing business loss.

- **Information Backup**

a. Information backup and restoration procedures shall be established and implemented by IT and Administration department to ensure the availability of business information;

b. Based on the criticality, business continuity and legal requirements, systems shall have a backup type (full) & schedule (daily/monthly) fixed. The frequency and type of backup shall be defined for each production system;

c. Backup storage location shall have appropriate level of protection consistent with the standards applied at the production systems;

d. Backup media shall be kept in godown in a fireproof cabinet with proper physical access controls.

e. Backup media shall be handled in accordance with the classification of the data stored on it; &

f. Backup operators shall store backup logs with appropriate access rights assigned to them. The backup operator shall carry out a log analysis for all failed backups.

- **Logging and Monitoring - Event Logging**

a. IT department shall ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored; &

b. It shall be ensured that the system administrators do not have permissions to erase or de-activate logs of their own activities.

c. Logging shall be enabled in all systems (which require monitoring) to log all critical events like success and failed logon/logoff attempts.

d. Adequate controls shall be established to protect the logs against tampering.

e. Automated systems shall be established to analyze the logs and alert of any suspicious activity.

- **Management of Technical Vulnerabilities**
  a. The IT department shall identify and document all technical vulnerabilities of information systems and evaluate the exposure to such vulnerabilities. Appropriate measures shall be taken to mitigate the associated risks;
  b. IT department shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability assessment and vulnerability closure;
  c. IT department shall ensure identification, documentation and remediation of technical vulnerabilities which arise across the following but not limited;
     - ✓ Operating systems
     - ✓ Databases
     - ✓ Network devices
     - ✓ Third-party procured software
  d. The vulnerabilities identified shall be addressed and remediated to the extent possible.

- **Restriction on Software Installation**

  The IT department shall define and ensure enforcement on which types of software shall be installed by users on the computer systems. The principle of least privilege shall be applied. If granted certain privileges, users shall have the ability to install software. **Safex Group** shall identify what types of software installations are permitted *(e.g., updates and security patches to existing software)* and what types of installations are prohibited *(e.g., software that is only for personal use and software whose lineage with regard to being potentially malicious is unknown or suspect)*. These privileges shall be granted having regard to the roles of the users concerned.

- **Patch Management**
  a. Installing system patches shall follow the change management procedure. New releases/ patches pertaining to the operating system shall be tested before being implemented in the operational environment to ensure that there is no adverse impact on operation, application controls or security.
  b. The application controls shall be reviewed to ensure that they have not been compromised by the operating system changes; &
  c. It shall be ensured that notification of operating system changes is provided in time so that appropriate tests and reviews are done before implementation.

14. Information Security Incident Management

All security breaches or attempts to breach and all discovered security weaknesses in information systems and processing facilities shall be reported at **Insert Email ID**. The information security incident management ('ISIM') process shall ensure that all reported security breaches or weaknesses are responded promptly, and actions taken to prevent recurrence.

The ISIM section defines the controls required for early detection, reporting and resolution of security incidents and weaknesses. Incidents include but are not limited to:
a. Physical security breach of **Safex Group** premises;
b. Loss of **Safex Group** owned information;
c. Loss or theft of **Safex Group** assets;
d. Malware *(virus)*;
e. Misuse of **Safex Group** systems, etc.

- **Responsibilities and Procedures**
  a. Roles and responsibilities shall be defined to ensure effective and prompt resolution of information security incidents;

b. Procedures shall be established to handle different type of information security incident such as but not limited to, information system failure and loss of service, breaches in confidentiality and integrity, misuse of information systems etc.; &

c. Procedures shall be established to recover from security breaches and correct system failures and shall ensure that all emergency actions taken are documented and reviewed by **Safex Group**'s management in an orderly manner.

- **Reporting Information Security Events**

a. All employees and third-party users shall report any security incident/ breach or weakness at **Insert Email ID**

b. Employees and third-party users shall be made aware of the possible security incidents that could impact the information assets of **Safex Group** and their responsibilities for reporting the incidents or weaknesses they observe;

c. Employees and third-party users shall not attempt to exploit any suspected security weakness. It shall be interpreted as a potential misuse of information system and shall result in disciplinary action for the individual;

d. Malfunction or other anomalous system behavior may be an indicator of a security attack or actual security breach and shall be always reported as information security event; &

e. All the security breaches shall be always reported as information security events and shall result in disciplinary action for the individual.

f. The Information Technology (IT) department shall establish an Incident response procedure and communicate the same to all departments and users.

g. All security related incidents shall be logged and prioritized based on potential impact to **Safex Group'** information systems.

h. Escalation mechanism and matrix shall be established to communicate incidents to **Safex Group** management.

First level	Asst. Manager (I.T)
Second level	Sr. Manager/A.V.P (I.T)
Third level	Group Director

15. **Information Security Aspects of Business Continuity Management**

Application systems and business processes that are critical to the business shall be planned for continuity of operations in the events of business disruptions. The cost effectiveness and fitness for the purpose of countermeasures to be implemented shall be considered and continually reviewed as part of normal management responsibilities.

The interruptions could be due to natural or manmade disasters, or technology incidents which might translate into disasters. **Safex Group** management shall:

a. Define the methodology of business continuity framework at **Safex Group;**

b. Implement controls that are required to ensure the availability and security of information and information systems;

c. Ensure the availability of services and information security requirements for critical business process, systems, and applications; &

d. Communicate the occurrence of a business interruption event internally as well as externally.

- **Information Security Continuity**
  a. A thorough risk assessment shall be planned for all assets required for business continuity, considering all the events that can cause disruption to the business processes. The considered events shall include, but are not limited to, man-made error/ disaster, natural disaster, and technical failure; &
  b. The AVP (IT) and the functional heads shall ensure that critical business processes, systems, applications are identified and prioritized on an annual basis. The major business processes shall cut across multiple departments.
  -
- **Availability of information processing facilities**
  a. **Safex Group** shall identify business requirements for the availability of information systems;
  b. If the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures shall be considered; &
  c. Redundant information systems shall be tested to ensure the failover from one component to another component works as intended, wherever applicable.

16. Compliance

Compliance with legal, statutory, contractual obligation and/ or security requirements is of extreme importance. All business functions shall be committed to adhere to these requirements and aim to embed a compliance culture in the organization. The objectives of this section of the policy are:

- **Identification of Applicable Legislation and Contractual Requirements**
  a. A list of all relevant statutory, regulatory, and contractual information security requirements shall be identified and maintained; &
  b. The list of applicable legislations shall be reviewed and approved at least once a year or whenever there is a change in any statutory, contractual obligations.

- **Intellectual Property Rights**
  a. Intellectual property is the original expression that derives its intrinsic value from a creative idea and shall be considered as a critical asset. The classification and ownership of intellectual property rights shall be included in all the contracts; &
  b. **Safex Group** will comply with the software license policy for all the procured software's.

- **Protection of Records**
  a. **Safex Group**'s important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements;
  b. The relevant business, legal and regulatory requirements shall be identified and documented for storing the information marked as 'Confidential' or 'Restricted';
  c. Identification of sensitive personal data *(if any)* shall be done as per the applicable laws and regulations;
  d. Data that is no longer required for business, legal and/ or regulatory purpose shall be securely disposed of;
  e. Sensitive information such as books of accounts, etc. shall be shared with government bodies, within the timelines defined in the applicable laws and regulations after appropriate authorizations; &
  f. Consideration shall be given to the possibility of deterioration of media used for storage of records.

Compliance with Security Policies and Standards

Functional heads shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with **Safex Group**'s security policies and standards.

17. Enforcement

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:

a. Loss of access privileges to information assets

b. Termination of employment or contract

c. Other actions deemed appropriate by Management

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

18. Document References

Document/ Form No.	Title
Tracker	Review of Access Rights
Tracker	IT Asset Under BYOD
Tracker	Warranty Tracker
Tracker	Annual Restoration Testing Drill
Tracker	Annual Operation Plans

Suresh
01/04/23