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

Identity & Access Management

Suresh
01/04/23

Safex Group

Identity & Access Management Policy

1. Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Identity and Access Management Policy
2.	Document Code	ITIAM01
3.	Date of Release	01-04-2023
4.	Document Version No.	1.0
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	-		
2			
3			

Suresh
01/04/23

2. Purpose

The purpose of the Safex Group Identity and Access Management Policy is to establish the requirements necessary to ensure that access to and use of Safex Group Information Resources is managed in accordance with business requirements, information security requirements, and other Safex Group policies and procedures.

3. Scope

The Safex Group Identity and Access Management Policy applies to individuals who are responsible for managing Safex Group Information Resource access, and those granted access privileges, including special access privileges, to any Safex Group Information Resource.

4. Policy

Access Control

- Access to Safex Group Information Resources must be justified by a legitimate business requirement prior to approval.
- Safex Group Information Resources must have corresponding ownership responsibilities identified and documented.
- Access to confidential information is based on a "need to know".
- Confidential data access must be logged.
- Access to the Safex Group network must include a secure log-on procedure.
- Workstations and laptops must force an automatic lock-out after a predetermined period of 5 minutes.
- Documented user access rights and privileges to Information Resources must be included in disaster recovery plans, whenever such data is not included in backups.

Account Management

- All personnel must sign the Safex Group Information Security Policy Acknowledgement before access is granted to an account or Safex Group Information Resources.
- All accounts created must have an associated, and documented, request and approval.
- Segregation of duties must exist between access request, access authorization, and access administration.

Delegation of Authorities matrix for access management:

Activity	Designation	Responsibilities
New access request / Revocation request of access right/ Modification request of access right	Sr. Manager IT/Asst. Manager IT	Raises a request.
Approval for new access request/revocation of access right/modification of access right	IT Head	Approves the request.
Review of approval for new access request/approval for	IT Head	Review the approval.

revocation of access right/approval for modification of access right		

- Information Resource owners are responsible for the approval of all access requests.
- User accounts and access rights for all Safex Group Information Resources must be reviewed and reconciled at least annually, and actions must be documented.
- All accounts must be uniquely identifiable using the username assigned by Safex Group IT and include verification that redundant user IDs are not used.
- All accounts, including default accounts, must have a password expiration that complies with the Safex Group Authentication Standard.
- Only the level of access required to perform authorized tasks may be approved, following the concept of "least privilege".
- Whenever possible, access to Information Resources should be granted to user groups, not granted directly to individual accounts.
- Shared accounts must not be used. If share accounts are required, documented approval should be obtained from the designated Information Resource owner.
- If required, user account set up for third-party cloud computing applications used for sharing, storing and/or transferring Safex Group confidential or internal information must be approved by the resource owner and documented.
- Upon user role changes, access rights must be modified in a timely manner to reflect the new role.
- Creation of user accounts and access right modifications must be documented and/or logged.
- Any accounts that have not been accessed within a defined period will be disabled.
- Accounts must be disabled and/or deleted in a timely manner following employment termination, according to a documented employee termination process.
- System Administrators or other designated personnel:
  1) Are responsible for modifying and/or removing the accounts of individuals that change roles with Safex Group or are separated from their relationship with Safex Group.
  2) Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.
  3) Must have a documented process for periodically reviewing existing accounts for validity.
  4) Are subject to independent audit review.
  5) Must provide a list of accounts for the systems they administer when requested by authorized Safex Group IT management personnel.
  6) Must cooperate with authorized Safex Group Information Security personnel investigating security incidents at the direction of Safex Group executive management.

Administrator/Special Access

- Administrative/Special access accounts must have account management instructions, documentation, and authorization.
- Personnel with Administrative/Special access accounts must refrain from abuse of privilege and must only perform the tasks required to complete their job function.
- Personnel with Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).

- Shared Administrative/Special access accounts should only be used when no other option exists.
- The password for a shared Administrative/Special access account must change when an individual with knowledge of the password changes roles, moves to another department or leaves Safex Group altogether.
- In the case where a system has only one administrator, there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency.
- Special access accounts for internal or external audit, software development, software installation, or other defined needs, must be administered according to the Safex Group Authentication Standard.

Authentication

- Personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed and implemented according to the following Safex Group rules:
  1) Must meet all the requirements established in the Safex Group Authentication Standard, including minimum length, complexity, and rotation requirements.
  2) Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
  3) Should not include common words, such as using dictionary words or acronyms.
  4) Should not be the same passwords as used for non-business purposes.
- Password history must be kept to prevent the reuse of passwords.
- Unique passwords should be used for each system, whenever possible.
- Where other authentication mechanisms are used (i.e., security tokens, smart cards, certificates, etc.) the authentication mechanism must be assigned to an individual, and physical or logical controls must be in place to ensure only the intended account can use the mechanism to gain access.
- Stored passwords are classified as confidential and must be encrypted.
- All vendor-supplied default passwords should be immediately updated, and unnecessary default accounts removed or disabled before installing a system on the network.
- User account passwords must not be divulged to anyone. Safex Group support personnel and/or contractors should never ask for user account passwords.
- Security tokens (i.e., Smartcard) must be returned on demand or upon termination of the relationship with Safex Group, if issued.
- If the security of a password is in doubt, the password should be changed immediately.
- Administrators/Special Access users must not circumvent the Safex Group Authentication Standard for the sake of ease of use.
- Users should not circumvent password entry with applications remembering embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Safex Group IT Management.
- If a password management system is employed, it must be used in compliance with the Safex Group Authentication Standard.
- Computing devices should not be left unattended without enabling a password protected screensaver or logging off the device.
- Safex Group IT Support password change procedures must include the following:

1) authenticate the user to the helpdesk before changing password.
2) change to a strong password.
3) require the user to change password at first login.

- In the event that a user's password is compromised or discovered, the password must be immediately changed, and the security incident reported to Safex Group IT support.

Remote Access

- All remote access connections to the Safex Group networks will be made through the approved remote access methods employing data encryption and multi-factor authentication.
- Remote users may connect to the Safex Group networks only after formal approval by the requestor's manager or Safex Group Management.
- The ability to print or copy confidential information remotely must be disabled.
- Users granted remote access privileges must be given remote access instructions and responsibilities.
- Remote access to Information Resources must be logged.
- Remote sessions must be terminated after a defined period of inactivity.
- A secure connection to another private network is prohibited while connected to the Safex Group network unless approved in advance by Safex Group IT management.
- Non- Safex Group computer systems that require network connectivity must conform to all applicable Safex Group IT standards and must not be connected without prior written authorization from IT Management.
- Remote maintenance of organizational assets must be approved, logged, and performed in a manner that prevents unauthorized access.

Vendor Access

- Vendor access must be uniquely identifiable and comply with all existing Safex Group policies.
- External vendor access activity must be monitored.
- All vendor maintenance equipment on the Safex Group network that connects to the outside world via the network, telephone line, or leased line, and all Safex Group Information
- Resource vendor accounts will remain disabled except when in use for authorized maintenance.

5. 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.

Sukti
01/04/23