Safex Group

Data Breach Notification Procedure

Suresh
01/04/23

Safex Group

Data Breach Notification Procedure

1. Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Data Breach Notification Procedure
2.	Document Code	ITDBN01
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

Safex Group. (hereinafter referred as "Safex Group" or "the Company" processes personal data hence it becomes vital that appropriate measures are in place to protect such data against accidental or unlawful destruction, loss, alteration, unauthorised access, or disclosure. Applicable Data Privacy Regulations specify that all breaches (except those that are 'unlikely to result in a risk to the rights and freedoms of natural persons) should be reported.

3. Scope

This procedure applies to all personnel (employees, contractual third parties and partners) and departments who are involved in handling personal, company and client information.

In particular, this procedure applies to those who are responsible for classifying and protecting Safex Group' data, as defined by the Information Security Roles and Responsibilities.

4. Objective

The objective of this procedure is to respond to the unauthorized disclosure of data, including personally identifiable information ("Personal Data") of its customers, vendors, employees, job applicants or any other persons whose data resides within Safex Group' network and machines.

This procedure is designed to set out general principles and actions that should be followed to ensure an effective approach is in place for reporting a personal data breach and to further ensure that:

- Data breaches are detected, reported, and monitored on a regular basis;
- Incidents are accessed and responded to appropriately;
- Appropriate actions are taken to minimise the impact of a breach;
- Relevant breaches are reported to the relevant supervisory authority within the time frame under applicable data privacy regulation;
- Improvements are made to prevent recurrence of the breach; &
- Lessons learnt are communicated to the relevant stakeholders.

5. Terms & Definitions

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

Personal data	Personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Supervisory authority	An independent public authority which is established by a State/ Country pursuant to applicable Data Privacy Regulation.

6. Notification of Personal Data Breach to Supervisory Authority

- Safex Group determines if the supervisory authority needs to be informed in the event of a breach. If the risk to the aggrieved party is likely from the breach, Safex Group shall report the personal data breach to the relevant supervisory authority within 72 hours (including weekends) after having become aware of the breach.
- Safex Group shall provide the following information to the supervisory authority:
  a) Date and time when the breach was occurred;
  b) Nature of personal data involved in the breach;
  c) Categories and approximate number of individuals concerned;
  d) Categories and approximate number of personal data records concerned;
  e) Name & contact details of the contact point where information can be obtained;
  f) Likely consequences of the personal data breach; &
  g) Measures taken / proposed to be taken to address the personal data breach.
- If it is not possible to provide all of the necessary information at the same time, Safex Group shall provide the information in phases without delay.

7. Notification of Personal Data Breach to Aggrieved Party

- If a personal data breach is likely to result in high risk to the rights & freedoms of the aggrieved party, Safex Group shall inform the data subjects affected within 72 hours (including weekends). The notification to the data subject describing the breach shall be in clear and plain language and shall contain at least the following information:
  a) Name & contact details of the contact point where information can be obtained;
  b) Likely consequences of the personal data breach; &
  c) Measures taken / proposed to be taken to address the personal data breach.
- If the breach affects a high volume of individuals and personal data records, Safex Group shall decide based on assessment the amount of effort involved in notifying each aggrieved party individually, and whether it will hinder Safex Group' ability to appropriately provide the notification within the specified time frame. In such a scenario, an appropriate method of public communication shall be adopted to inform those affected in an equally effective manner.

8. Responsibilities

- All users (whether employees, contractors, or third-party users) of Safex Group are required to be aware of and follow these procedures in the event of a personal data breach.
- All employees, contractors or third-party users are responsible for reporting any personal data breach to the A.V.P (I.T).

9. Enforcement

9.1 Procedure violations

- The indicators of compromise and violation of procedure shall be treated as per the guidelines mentioned in the Information Security Policy and the same needs to be reported as in information security incident.
- Disciplinary and legal action shall be taken against any employee or third-party contractor who is found guilty of a breach of any instructions or guidelines of this procedure.

9.2 Procedure exceptions

- Any exceptions to this procedure have to be formally approved by the Group Director. All the exceptions shall be tracked by Safex Group' IT services team in IT exceptions request tracker. The exception request shall follow the below mentioned approval matrix.

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

10. Annexure – Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach, please notify your supervisor immediately, complete Section 1 of this form and email it to the Safex Group' IT department at it@safexchemicals.com.

Section 1: Notification of data security breach

Date incident was discovered:	
Date(s) of incident:	
Date of reporting incident to supervisory authority	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (Email, Address, Telephone Number):	
Brief description of incident or details of information lost:	
Number of party/ persons affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of action taken at time of discovery, if any?	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of severity

Details of the IT system, equipment's, devices, records involved in the security breach. Details of information loss.	
What is the nature of lost information	
How much data is lost? If laptop is lost/ stolen	

How recently is laptop backed up onto central IT system?	
Is the data bound by contractual security arrangement?	
Please provide details for any information that falls into following categories: • High risk personal data • Special category personal data relating to living, identifiable information: a) Racial/ethnic origin b) Political opinion/religious belief c) Genetics d) Biometric e) Health f) Sexual orientation	
Any information that could be used to commit identity fraud such as personal bank account and financial information; national identifiers (e.g., Passport)	

Section 3: Action taken

Incident number		
Report received by		
Date		
Action taken by responsible officer/s		
Reported to DPO (if appointed)	If yes, date of notification?	
Notification to supervisory authority	If yes, date of notification?	
Notification to aggrieved party	If yes, date of notification?	

SURESH
01/04/23