Shreetron India Limited

Data Breach Policy

Revision History

Version	Issue Date	Prepared By	Approved By	Changes
1.0	02.04.2021	vaneet Soni	A P Panwar	Initial Draft

1. Scope:

This policy covers all computer systems, network devices, and any additional systems and outputs containing or transmitting AUA name Protected data or (AUA name) Sensitive data.

2. Purpose:

The purpose of this policy is to provide a process to report suspected thefts involving data, data breaches or exposures (including unauthorized access, use, or disclosure) to appropriate individuals; and to outline the response to a confirmed theft, data breach or exposure based on the type of data involved.

Shreetron India Limited

3. Data Breach Policy

Reporting of suspected thefts, data breaches or exposures:

1. Any individual who suspects that a theft, breach or exposure of (AUA name) Protected data or (AUA name) Sensitive data has occurred must immediately provide a description of what occurred to respective Project Manager and Management. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the team will follow the appropriate procedure depending on the class of data involved.
2. If the incident is a suspected theft, Project Manager and Management shall determine whether a local law enforcement agency should be contacted based on the location and details of the incident.
3. Confirmed theft, data breach or exposure of (AUA name) Protected data or (AUA name) Sensitive data:
4. As soon as a theft, data breach or exposure containing (AUA name) Protected data or (AUA name) Sensitive data is identified, the process of removing all access to that resource will begin as soon as possible. If the information is available on a site outside of (AUA name), that site will be contacted to have the information removed as soon as possible.
5. The management shall form a response team to handle the breach or exposure. The team will include members from Management and respective Project Manager. Additional departments shall be included based on the type of data involved.
6. The Management will also determine if it is also appropriate to report relevant law enforcement agencies based on where the theft occurred.

---- End of the document ----