Incident Management& Privacy Policy

Policy Statement

Eagle Cabs is committed to providing a safe workplace for all personnel, contractors and vendors, sub-contractors. We are committed to establishing a formal process to report and investigate all workplace accidents/incidents and near miss occurrences. This process includes identifying contributing factors of the accident/incident or near miss and making the necessary recommendations to prevent a recurrence. requirements for meeting state, city, or provincial laws/regulations, related to security, confidentiality, processing integrity, disposal and protection of the personally identifiable information.

Purpose

To provide guidelines as far as reasonably practicable to establish the process for reporting, investing and applying appropriate control measures when an accident, incident or near miss occurs. The aim is to provide safe systems of work along with a safe working environment for all Vendor Name sites.

Definitions

Privacy Event means a breach of confidentiality, infringement, or violation of any right to privacy including, but not limited to, a breach of your privacy policy, breach of a person's right of publicity, false light, intrusion upon a person's seclusion, or public disclosure of a person's private information.

Scope

This policy applies to the entire Company, Faculty, staff, and all units, Third-party vendors, our sub vendors and contractors, who collect, process, share or maintain Company institutional data, whether managed or hosted internally or externally and personally, owned devices of employees of the company that access or maintain sensitive institutional data.

Our Responsibilities

Eagle Cabs has implemented this policy to handle information security incidents to reduce impact on the maintenance, confidentiality & integrity, and availability of the company's systems, applications, and data by following the below

- Modifying the impact of all the system security incidents.
- Protecting, preserving, and making better & substantial usage of all information regarding the incident or disclose for analysis and notification.
- Make sure that all the employees and sub-contractors are aware of their roles & duties for handling system security incident.
- Identifying the sources and underlying causes of system security incidents and unauthorized disclosures to aid in reducing their future likelihood of occurrence.

Investigation, Remedies and Reporting

Company's system users must report all security incidents information to their IT security provider tie-up with the company.
Any serious information security incident must be immediately reported to Management of the company.

The employees of the company may not release any information, any devices or media to any outside individuals / sub-contractors / entity without any prior notification of the company to avoid / violations of the company's policy

If any Incidents occurs in any activity related to the company or client, in regards to the handling and management of information in physical format or logical databases that store both client and company data must be bring to the notice of the company
The management will record the security incident containing Type of Incident, Description of the Incident, Date and time of the notification, User reporting the incident
The management will retain relevant records and evidence pertaining to all serious incidents till its resolution and solution
If any Incident is observed / detected, it will be passed to an expert team of dedicated persons, who has supreme knowledge in the concerned department.

Investigation will be completed by seizing the laptop or any other device issued to employee / subcontractor for the use of the company immediately after identifying an incident

The management with the responsible team displays the activities to be performed for rectification / correction of the incident.

The Management of the company shall report the incident and resolution to the impacted client, if any via mail/telephonic communication within 24 hours.

Control Mechanism

a. Anti-Virus & Anti-Malware has been installed in all the PCs; Laptops & Servers related to the company
b. Only authorized employees are permitted to entry with their key cards. Unauthorized persons are restricted to enter in the premises.
c. Information Security team conducts audits from time to time and Training is provided on regular basis for all the employees as well as management.