iGROW
Driving Inclusivity and Growth Together

LEAKAGE OF CLIENT INFORMATION

Leakage of client information

Confidential material, including banking details, names and addresses and other identifying details, is regularly entrusted to businesses of all kinds (PII). It is a serious obligation that grows harder over the years to keep this data protected from individuals who would misuse it.

Data breaches can have a catastrophic impact on the activities and credibility of your business. Huge amounts of money could be lost as a result of the interruptions brought on by a data theft as you try to determine what went wrong and how much harm was done.

We at our company, have high importance to paying absolute attention to prevent any data leakage or theft and if found, we believe in taking harsh judgements, penalties and judicial help against the person or group responsible for such act. It is our top priority to prevent even a minimal leakage of client's information and data

We as a responsible company have built following measures to mitigate the risk of data leakage. Some of these measures are:

1. **Cybersecurity Trainings:** Another important aspect we find valuable is adequate training of all the personnel in matters relating to cybersecurity. This awareness is very crucial so that employees don't fall in trap and not become a part of any wrongdoing intentionally or unintentionally.

To prevent employees from succumbing for such assaults, it can be quite helpful to educate them on cybersecurity awareness in order to identify spoofing efforts as well as other cyber-attack tactics. Additionally, it can assist them in understanding what they should do in the event of an assault, enhancing your business's total capacity to recognise and react to such assaults.

2. Cleaning Data Storage: We Make sure that privacy information is really not stored on every desktop, cell phone, and USB device in the business is among the greatest strategies to prevent data leaks. We n ever keep confidential material, including the personally identifiable information (PII) of our clients, on a worker's workstation or external drive, which could be quickly taken during an assault.

It can be more secure to keep that information in a centralised, secure location (like a well-defended database) that staff members with the appropriate user registration can view remotely over a private virtual network (VPN).

3. Revoking Access as soon as employee leaves the company: Whenever we terminate an employee, or whenever there is an exit of an employee from a company, we make sure that we revoke all the company access which was granted to the employee, regardless of the terms on which they are leaving the company.

The confidentiality of the information in the company can indeed be extremely at risk as a result of departing personnel. When an employee's term ends, they have less incentive to properly uphold data security protocols if they're departing on amicable terms. We avoid any desire to abuse privilege by swiftly disabling a dismissed employee's connection to our most confidential documents. Even if the person is thought to be 100 percent reputable, it's crucial to approach all employees equally to reduce hazards.

4. **Protecting Endpoints:** We focus to establish security systems like firewall, antivirus systems etc to minimize the exposure of data leak. These however do not eliminate the risk but minimize it. This security check is enabled at each and every entry and exit point of data so that it falls in complete control and security.

Accelerating Excellence

& Sustainable Economic Growth

Follow us:

Facebook

Instagram

Twitter

LinkedIn