PERSONAL INCIDENT RESPONSE PLAN

This personal 入射 response plan is prepared to ensure that each associate is prepared to report Data Breach incidents in a disciplined and timely manner. A Data Privacy **Breach** leads to the **Accidental** or **Unlawful Disclosure**, **Access**, **Alteration** or **Destruction** of Personal Data (PI, SPII) **Transmitted**, **Stored** or otherwise **Processed**. The objective is to ensure that we as an organization respond to data breaches meeting the regulatory requirement of 72 hours as a standard. All associates should keep this plan handy as reference in event of knowing off or being intimated about a data security breach. The most common scenarios for breach intimation are:

- **Customer Reports a potential Data Breach to Sales Team**: The customer representative communicates details of a potential breach to the Tech M Sales representatives.
- **Customer Reports a potential Data Breach to a Delivery Leader**: The customer delivery organization reports an identified data breach arising due to a compromise by a TechM associate, system or process being delivered to the customer to a project manager or senior delivery leader
- **Delivery Associate Identifies a Data Breach 入射**: An associate discovers that there has been a data breach in the course of his normal work.
- **Receive an Extortion Call or Email from a Hacker**: An associate receives a message from a malicious actor demanding ransom to safeguard the personal data in custody of the malicious actor.
- **You suspect that your laptop / desktop is infected with a malware or you have clicked on a suspicious email**: An associate suspects that his credentials have been compromised or that there is suspicious activity on the desktop / laptop which may degrade the system performance or lead to a Data Breach.

INCIDENT RESPONSE ACTION

The key goal of incident response is to ensure that the right teams in Tech Mahindra are alerted immediately such that the breach can be contained, investigated and adequately reported to stakeholders. For the purpose of security investigation, the company has designated individuals with specific responsibility to manage these incident as part of regulatory requirements and good security practice.

Associates need to follow the response plan given below based on their role.

Action Plan	Customer Reports a potential Data Breach to Delivery or Sales	Delivery Associate Identifies a Data Breach Incident	Receive an Extortion Call or Email from a Hacker with Project PI / SPII	Suspect that your laptop or desktop with PI / SPII is infected with malware or you have clicked a link in a suspicious email.
1. Raise an Incident in the Incident Management System Portal. EASY (https://easy.techmahindra.com/easylogin.aspx) → Information Security → Incident Management System **2. Notify TechM Data Privacy Protection Officer (DPO) at DPO@techmahindra.com** **3. Email Notification to SBU Head**	✓	✓	✓	✓

IMPORTANT POINTS TO REMEMBER

1. Breach information shall only be communicated to – SBU Head, DPO, CISO, Incident Management Team.
2. The SBU Head or CISO would inform the Customer.
3. Affected parties would be informed by the DPO or Customer DPO
4. All **External Communication** would be handled by the **Head - Marketing**

#	Do	#	Don't
1	Notify immediately. Delays can lead to penalty and / or legal action by authorities	1	Do not Distribute the email to distribution lists or include associates in the mail chain.
2	Ensure PII or SPII is masked before forwarding or ensure mail is encrypted.	2	Do not Disclose details of the incident and investigation process
3	Disclose all information you are aware of and honestly.	3	Do not Speak to Media, colleagues or external parties, Post on Social Media or Converse in Public Places. Maintain strict confidentiality
4	Seek advice and / or authorization from TechM Data Privacy Protection Officer (DPO) if in Doubt.	4	Do not Click on any links or open attachments with supposedly confidential information.
5	Take best effort to notify TechM Authorized Personnel as in the Data Response Plan	5	Do not Delete any evidence or information unless directed to.

ACTION TAKEN POST INCIDENT REPORTING

Investigation is initiated to review evidence, identify if it is a breach and notify or brief stakeholders. The DPO reviews the investigation report and engages with the corresponding Business Unit Leaders. Incident Analysis is conducted to identify the source and root cause.

Cyber Simulation Exercises: Being prepared is important. There would be Data Breach Response Tests conducted simulating the scenarios presented in this document. These will be pre-scheduled, as well as surprise tests across all associates of Tech Mahindra. An advanced end to end exercise including Incident simulation, Response, Investigation, Reporting, Communication and Media Integration shall be conducted too.

QUICK LINKS

Business Management System → Support Function Processes → Business Support → ISG →Information Security Incident Management Policy (ISG-PO003)

Tech Mahindra DPO Appointment - https://www.techmahindra.com/media/News-and-Updates/Statement-on-compliance-with-the-GDPR-for-TechMahindra.aspx

EASY → https://easy.techmahindra.com/easylogin.aspx → Information Security → Incident Management System