timeTec

# DATA BREACH RESPONSE POLICY

| | | | |
|---|---|---|---|
| **Document Name:** | **Data Breach Response Policy** | | |
| **Current Version:** | V1.2 | | |
| **Prepared by:** | Barry Chai, COO | **Signature:** | |
| **Approved by:** | Daryl Choo, CTO | **Signature:** | |
| **Last Updated:** | 27th October 2017 | | |
| **Confidentiality Level** | Confidential | | |

# Data Breach Response Policy

## 1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

TimeTec Cloud Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how TimeTec Cloud's established culture of openness, trust and integrity should respond to such activity. TimeTec Cloud Information Security is committed to protecting TimeTec Cloud's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

## 1.1 Background

This policy mandates that any individual who suspects that a theft, breach or exposure of TimeTec Cloud Protected data or TimeTec Cloud Sensitive data has occurred must immediately provide a description of what occurred to the CTO/COO or IT Operation. The CTO 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 CTO will follow the appropriate procedure in place.

## 2.0 Scope

This policy applies to all who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information of TimeTec Cloud members.

## 3.0 Policy Confirmed theft, data breach or exposure of TimeTec Cloud Protected data or TimeTec Cloud Sensitive data

As soon as a theft, data breach or exposure containing TimeTec Cloud Protected data or TimeTec Cloud Sensitive data is identified, the process of removing all access to that resource will begin.

The CTO will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Operation
- Development Team
- Finance (if applicable)
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the CTO
- Top Management if deemed necessary

**Confirmed theft, breach or exposure of TimeTec Cloud data**

The CTO will be notified of the theft, breach or exposure. IT, along with the incident response team, will analyze the breach or exposure to determine the root cause.

**Develop a communication plan.**

Work with TimeTec Cloud human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

### 3.2 Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the TimeTec Cloud community that have primary responsibility for maintaining any particular information resource. TimeTec Cloud HOD's are the appointed Sponsors in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- IT Operation Team would provide administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the TimeTec Cloud community to the extent they have authorized access to information resources, and may include staff, contractors, consultants, interns, and temporary employees.
- The Incident Response Team shall be chaired by CTO

## 4.0 Enforcement

Any TimeTec Cloud personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment and legal action. Any third party partner company found in violation,  legal action may be instituted.

## 5.0 Definitions

**Encryption or encrypted data** – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;
**Plain text** – Unencrypted data.
**Information Resource** - The data and information assets of an organization, department or unit.
**Safeguards** - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.
**Sensitive data** - Data that is encrypted or in plain text.

## 6.0 Revision History

| **Version** | **Date of Change** | **Prepared by** | **Summary of Change** |
|---|---|---|---|
| **1.0** | 1st August 2017 | Barry Chai | 1st Baseline |
| **1.1** | 13th August 2017 | Barry Chai | Temporarily removed the following until further notice (for future implementation)<br>*“**Working with the Insurer***<br>*As provided by TimeTec Cloud, the insurer will be provided access to in order to determine how the breach or exposure occurred and analyze the breach or exposure to determine the root cause.”* |
| **1.2** | 27th October 2017 | Barry Chai | Edit to indicate incident reporting to “CTO only” to “CTO/COO” or IT Operation. |