DATA BREACH POLICY

Background

The Thailand PDPA is based around eight principles of handling of personal data. The Thai-Chinese International School (TCIS) must comply with all eight principles as an organization: otherwise, we will be in breach of the PDPA. We understand that the principles give people specific rights in relation to their personal information and place certain obligations on those organizations that are responsible for processing it.

The eight principles are:

- Personal data must be processed lawfully.
- Personal must be collected for specified, explicit and legitimate purposes.
- Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Personal data must be ensured accurate and kept up to date.
- Personal data must be kept for no longer than is necessary.
- Personal data must be processed in accordance with the individual's rights.
- Personal data must be kept secure.
- Personal data must not be transferred to third countries which do not provide adequate protection.

Aim

The PDPA requires that we must take appropriate measures against unauthorized or unlawful processing and against accidental loss, destruction of or damage to personal data. This policy sets out how we deal with a data security breach.

What is a personal data breach?

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted, or disclosed if someone accesses the data or passes it on without proper authorization; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Data Breach Types

The CIA Triad

Confidentiality

Confidentiality involves the efforts of an organization to make sure data is kept secret or private. To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data—whether intentional or accidental. A key component of maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to your business. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.

Integrity

Integrity involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable. For example, if your company provides information about senior managers on your website, this information needs to have integrity. If it is inaccurate, those visiting the website for information may feel your organization is not trustworthy.

Availability

Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization and the customers they serve. This means that systems, networks, and applications must be functioning as they should and when they should. Also, individuals with access to specific information must be able to consume it when they need to and getting to the data should not take an inordinate amount of time.

Actions to be taken in the event of a data breach or major incident involving personal data

1. Containment and recovery

The immediate priorities are to:

- Contain the breach.
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- To limit the scope.

Steps to take where personal data has been sent to someone not authorized to see it:

- Inform the recipient not to pass it on or discuss it with anyone else.
- Inform the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so.
- Explain to the recipient the implications if they further disclose the data; and
- Where relevant and high risk, inform the data subjects whose personal data is involved what has happened so that they can take any necessary action to protect themselves.

In the event of a data security incident or breach, staff must immediately inform the below Data Protection Officer (DPO).

Ms.Pichaya Sajawasunt
email: dpo@tcis.ac.th
T: 02-751-1201
M: 062-424-8247

The DPO will take the lead on investigating the breach. In the event where the DPO is absent for whatever reason, the following person will assume the lead.

Mr. Paisan Homhuan
email: dpo@tcis.ac.th
T: 02-751-1201
M: 098-552-9246

2. Recording and assessing the risk:

Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

Actions:

- The DPO will log into the privacy platform: https://pdpa.formiti.com
- Select Breach Management from the home screen.
- Complete the Breach Investigation form.

3. Notifying the PDPC and individuals, where relevant

Who is responsible?

The DPO is the point of contact for staff and the PDPC on this policy and on all matters relating to data protection.

The DPO is also responsible for notifying the PDPC and individuals (where applicable) of relevant personal data breaches.

What breaches do we need to notify the PDPC about?

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then we must notify the PDPC; if it is unlikely then we do not have to report it. If we decide we do not need to report the breach, we need to be able to justify this decision, and we should document it and add it to the company data breach register.

When to notify the PDPC and dealing with delays

Notifiable breaches must be reported to the PDPC without undue delay, but not later than 72 hours after becoming aware of it.

If we do not comply with this requirement, we must be able to give reasons for the delay.

In some instances, it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Where that applies, we should provide an interim report and provide updates in phases, as long as this is done without undue further delay.

Breach Incident Report

When reporting a breach, we will provide via our platform (which can download and print out) the following information:

- ❖ Description of the nature of the personal data breach including, where possible.
- ❖ Categories and approximate number of individuals concerned.
- ❖ Categories and approximate number of personal data records concerned.
- ❖ A description of the likely consequences of the personal data breach; and
- ❖ A description of the measures taken, or proposed to be taken, to deal with the personal data or to mitigate any possible adverse effects.

Individuals

Where notification to individuals may also be required, the DPO will assess the severity of the potential impact on individuals as a result of a breach and the likelihood of this occurring. Where there is a high risk, we will inform those affected as soon as possible, especially if there is a need to mitigate an immediate risk of damage to them.

Information to individuals

The DPO will consider who to notify, what we are going to tell them and how we are going to communicate the message. This will depend to a large extent on the nature of the breach but will include the name and contact details of our data protection officer (where relevant) or other contact point where more information can be obtained; a description of the likely consequences of the personal data breach; and a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The breach need not be reported to individuals if:

- ❖ We have implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach.
- ❖ We have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.
- ❖ It would involve disproportionate effort (in this case a public communication may be more appropriate).

In the case of a breach affecting individuals in different countries, we are aware that the PDPC may not be the lead supervisory authority. Where this applies, the TCIS should establish which international data protection authority would be the lead supervisory authority for the processing activities that have been subject to the breach.

Third parties

In certain instances, TCIS may need to consider notifying third parties such as the police, insurers, professional bodies, bank, or credit card companies who can assist in reducing the risk of financial loss to individuals.

Document all decisions

TCIS must document all decisions that we take in relation to security incidents and data breaches, regardless of whether or not they need to be reported to the PDPC.

4. Evaluate TCIS response and mitigation steps

We investigate the cause of any breach, decide on remedial action, and consider how we can mitigate it. As part of that process, we also evaluate the effectiveness of our response to incidents or breaches. To assist in this evaluation, we consider:

- What personal data is held, where and how it is stored
- Risks that arise when sharing with or disclosing to others
- This includes checking the method of transmission to make sure it is secure and that we only share or disclose the minimum amount of data necessary
- Weak points in our existing security measures such as the use of portable storage devices or access to public networks
- Whether or not the breach was a result of human error or a systemic issue and determine how a recurrence can be prevented – whether this is through better processes, further training, or other corrective steps
- Staff awareness of security issues and look to fill any gaps through training or advice
- The need for a Business Continuity Plan for dealing with serious incidents
- The group of people responsible for reacting to reported breaches of security

5. DPO Summary of steps for data breach

If the breach was contained or less serious:

- Download and complete the Breach Incident Report.
- Inform the Head of School of the breach.

- ❖ Decide if further training is needed.
- ❖ Record the breach on the school breach register.

If the breach is considered potential risk to the rights and freedoms of the data subject, this will be reported to the PDPC:

- ❖ Download the letter to the PDPC.
- ❖ Download the Breach Incident Report.
- ❖ Complete and submit the Breach Incident Report to the PDPC (remedial measure can be unavailable)

If the breach is considered high risk to the rights and freedoms of the data subject, this will be reported to both PDPC and data subject:

- ❖ Download the letter to the PDPC.
- ❖ Download the letter to go to the data subject.
- ❖ Download the Breach Incident Report.
- ❖ Complete the Breach Incident Report together with the remedial measures.
- ❖ Submit the Breach Incident Report to the PDPC and data subject.

Incidents should ***not*** be deleted from the breach register.

6. Review

This document is dated 04/03/2022 and will be reviewed by TCIS annually or upon development of the concerning technology to ensure effective and appropriate security measures, and in line with minimum legal requirements as prescribed by the laws and relevant authorities.