Data Incident and Breach Policy

Contents

Data Incident and Breach Policy

Introduction

This Data Incident and Breach Policy (“Policy”) sets out how Yokohama International School (“we”, “our”, “us”) will respond to any data security incidents and breaches.

The School Leadership Team is responsible for approving this Policy and related procedures.

The policy and procedures apply to all personal data we process regardless of the media on which the data is stored or whether it relates to past or present employees, students, parents, or other stakeholders (e.g. members of our Board of Directors).

The policy and procedures apply to all staff & faculty at Yokohama International School .

In accordance with our Yokohama International School Data Protection Policy, we commit to utilising this policy and procedure to ensure the correct and lawful treatment of personal data and to protecting the confidentiality and integrity of personal data.

Our Data Protection Officer (“DPO”) is responsible for reviewing this Policy on a regular basis. You can contact our Data Protection Officer by emailing dpo@yis.ac.jp.

Definitions

“Breach” can be broadly defined as a data 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 without consent. This can include if someone accesses the data or passes it on without proper authorisation, or if the data is made temporarily unavailable, for example, when it has been encrypted by ransomware.

“Data Security Incident” refers to an event that may compromise the integrity, confidentiality, or availability of an information asset. Data Incidents are situations which, upon further analysis, might be deemed by the School Data Incident Response Team to be a Data Breach (if the incident affects the confidentiality, integrity or availability of personal data) or might not. In short, every breach will necessarily involve a Data Security Incident, but not every Data Security Incident will result in a Breach.

“Security Event” means any reported or identified suspected Data Security Incident/Breach.
“Near Miss” means any Data Security Incident which did not result in a Breach.

Data Security Incident Response Team

Name	Contact Information
Craig Coutts, Head of School	couttsc@yis.ac.jp
Walter Pena, Head of Operations	penaw@yis.ac.jp
Matt Broughton, Data Protection Officer	dpo@yis.ac.jp
Aaron Marlin, Database Manager	marlina@yis.ac.jp

Akemi Watanabe, Facilities and Legal Affairs Manager	watanabea@yis.ac.jp

The members of the Data Security Incident Response Team shall meet quarterly to discuss trends and lessons learned as well as to discuss strategies and controls to better protect personal data entrusted to us.

General Policy

School personnel are required to report all data incidents to the Data Protection Officer. Even if the person was not directly involved in the loss or disclosure, they are obliged to report the matter immediately.

Upon reporting of a data incident, the Data Security Incident Response Team shall follow the Breach Incident and Breach Response Procedure, which is hereby incorporated by reference.

The Data Protection Officer shall keep the Head of Operations and Head of School updated on the status of all reported incidents and breaches under investigation via regular reporting. The determination regarding whether a particular incident or breach is considered closed (for reporting purposes) rests with the Head of School..

The Data Protection Officer is responsible for ensuring that the Incident Report Log, which is a catalogue of all reported incidents, is maintained and is up-to-date. This Log shall be reviewed regularly by the Data Protection Officer to ensure that we learn lessons from every incident by implementing appropriate measures to improve the operation of our data protection programme.

Data Security Incident and Breach Response Procedure

Procedure

Our Data Security Incident and Breach Procedure has five parts.
Step 1: Reporting of Incident (Background)
Step 2: Containment
Step 3: Incident Assessment
Step 4: Reporting
Step 5: Accountability and Response

Step 1: Reporting of Incident (Background)
School personnel are required to report all Security Events immediately after becoming aware of them. When in doubt about whether a particular situation may represent a data security incident/breach or not, staff are encouraged to report. Reporting shall consist of an email to the Data Protection Officer..

All reports of Data Security Incidents will be investigated to the fullest extent possible.

When new security events are reported, the Data Protection Officer shall keep accurate notes regarding the reported incident within the Incident Report Log (“Log”). Log entries shall include identifying what (if any) actions have been taken thus far, by whom, and the exact time and date of the incident and when it was reported.

Before progressing to the next step, the Data Security Incident Response Team shall confer to assess the reported Security Event. Specifically, the team shall make an initial determination regarding the credibility of the alleged Security Event to determine whether they should continue investigating the event or, on the other hand, if the report appears to be erroneous, false, and/or unsubstantiated.

Step 2: Containment

For those reported Security Events which appear as though they may be credible, the Data Security Incident Response Team shall conduct a root cause analysis to determine whether the root cause(s) of threat posed by the reported incident has been contained. If necessary, the school will secure outside data security/forensic experts to assist in this process.

If the Data Security Incident Response Team discerns during the course of that root cause analysis that the threat is ongoing, it will take steps to limit the compromise, for example working with relevant stakeholders to:

- Secure or disconnect affected systems;
- Secure affected records or documentation;
- Halt affected business processes;
- Pause any processes that may rely on exposed information;
- Change passwords on all affected systems and applications;
- Install additional security scans for malware; and
- Implement new security measures.

The Data Security Incident Response Team will also establish whether there is anything the school can do to recover any losses, e.g. physical recovery of data etc.

Step 3: Incident Assessment

After ensuring that the threat has been mitigated (as much as possible), the Data Security Incident Response Team shall meet to conduct an assessment of the reported Security Event. If, in the course of that meeting, the Data Security Incident Response Team determines that:

- a reported/identified security event does not represent a data incident, then it shall be logged in accordance with the “Data Breach Response” section of the Information Security Policy as a “near miss.” If the Data Security Incident Response Team identifies any steps necessary to mitigate any threats, then those steps shall be completed and recorded in the log as well; or
- a data incident did occur (or is still occuring) but it did not (or does not) involve any personal data, then we shall handle the incident in accordance with the process outlined in the “Incident Management Process” subsection of the “Data Breach Response” section of the Information Security Policy; or
- a data incident had occurred (or is occuring) which affected the confidentiality, integrity or availability of personal data by involving the loss, destruction, corruption or unlawful disclosure or access of personal data, then the incident shall be classified as a data breach and handled in accordance with the process outlined below. After handling the breach in accordance with the process below, we shall then follow the “Incident Management Process” subsection of the “Data Breach Response” section of the Information Security Policy.

Additionally, regardless as to the classification above, the Data Security Incident Response Team shall identify in the appropriate log whether the Security Event involved any personal data that is/was under the control of a third party (e.g. when the personal data is being stored by a processor or joint controller). If the incident occurred while the data was under the control of a third party, the Data Security Incident Response Team shall work with other parties, as necessary, to review the contract and determine the next course of action with that third party in accordance with this Procedure and the Data Security Incident and Breach Policy.

For all incidents and breaches, if it related to a breach of an information system, the Data Security Incident Response Teamshall assess and log:

- The type of information security incident which led to the breach (phishing, malware, password attack, zero-day exploit or denial of service)
- Which information systems were affected (application services, authentication services, internet access, file services, servers, storage, wireless services)
- Which information services were affected (access control, CCTV, email, finance, intranet, management or student information system, organisation website, printing, remote access)
- Whether a service desk ticket has been created to address the root cause and ensure that the breach is not ongoing
- What evidence can be provided to support the investigation of the incident

If the Data Security Incident Response Team determines that a breach occurred, it shall then assess and log:

- What types personal data is involved in the breach (e.g. phone numbers, names, photographs, etc.);
- The cause of the breach;
- The extent of the breach (i.e., how many individuals are affected);
- The potential harm to affected individuals caused by the breach;
- Whether the breach is still ongoing;
- Were vulnerable individuals affected (e.g., children or an individual who is unable to act on their own behalf for mental or physical reasons); and
- How the breach can be contained (including identification of which internal/external stakeholders need to be engaged, if any)
- any special category data is involved
- the number and type (e.g. students, parents) of data subjects impacted as well as the number of personal data records.
- if applicable, whether the school's records of processing involves a relevant processing activity
- Whether the school was acting as a controller or processor of the data in question
- For breaches, following an analysis of those issues, the Data Security Incident Response Team will investigate whether 1) the nature, sensitivity or volume of personal data affected, 2) the identification of individuals through exposure of their personal data, 3) the characteristics of the individual(s) affected by the breach, and/or 4) the number of individuals affected by the breach could lead to any of the following damages to those data subjects: damage or distress, reputational damage, financial loss, economic disadvantage, social disadvantage, confidentiality, identity theft.

Based on the results of those determinations, the Data Security Incident Response Team will then establish the overall level of risk present in the Breach by considering the likelihood and severity of the risk to people's rights and freedoms.

If the Data Security Incident Response Team determines that the Breach is unlikely to pose a risk to individuals' rights and freedoms, the team shall record in the Log that Breach as a Non-Reportable Breach. The team shall then continue to Step 5 of this Procedure.

For a Breach which is determined to pose a risk to individuals' rights and freedoms, the Data Security Incident Response Team shall record that Breach within the Log as a Reportable Breach and make a determination as to whether the risk posed to individuals is low or high.

For reportable breaches, the Data Security Incident Response Team will schedule a data incident investigation meeting. This meeting shall include other members of the Senior Leadership Team and Communications Department, as appropriate. The objective of this meeting is to define the incident, establish a plan to manage the impact as soon as possible (within 72 hours) and confirm any required communication. The Data Security Incident Response Team shall then continue to Step 4 of this Procedure.
See Appendix for sample data incident investigation meeting agenda

Step 4: Reporting
If the Breach is determined to be reportable in accordance with Step 3 (above), the Data Security Incident Response Team shall, notify the Personal Information Protection Committee (PPC) in accordance with APPI and fill out the relevant forms supplied by that agency.

Reporting is automatically legally required when:

- The data includes sensitive data.
- The data is likely to be used unlawfully and cause financial damages.
- It is likely that the breach was committed with an unlawful purpose.
- The data breach of more than 1,000 data subjects has occurred, or is likely to have occurred.

The following information must be provided to the regulator/supervisory authority:

- The categories and approximate number of individuals concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Data Protection Officer (if necessary) or another contact point;
- Description of the breach;
- Description of the measures taken; and
- Any other available information at the time of notice.

An initial report must be made immediately (within 3 to 5 days, according to the PPC guidelines), followed by a more detailed report within 30 days after becoming aware of the breach (or within 60 days in a case where it is likely that the breach was committed with an unlawful purpose

Where the Data Security Incident Response Team determines that a high risk to data subjects exists, the Team is responsible for notifying each individual that has been affected by the breach with the following information :

- A description of the breach;
- Likely consequences of the breach;
- Measures taken or proposed to be taken by the controller to address the breach;
- The name and contact details of the Data Protection Officer or other contact point; and
- Advice to individuals to protect themselves from possible adverse consequences of the breach, such as by resetting passwords or monitoring credit scores.

Communication to individuals affected should be via email, alternative methods of contacting individuals include postal mail or website notification.

Step 5: Accountability and Response
After completing any necessary containment steps (identified in Step 2) to stop any ongoing threat(s) and contacting any appropriate parties (as determined in Step 4), the Data Security Incident Response Team shall:

- Record all relevant information regarding the breach within the log including:
    - A summary of the incident
    - Proposed actions to be undertaken in response (specifically identifying who will be completing the actions and by when each action will be completed)
        - For reportable breaches, the proposed actions should include a recovery plan consisting of mitigating actions for each risk.
    - An identification of the assessment decision (near miss, non-reportable incident, reportable incident)
    - Any lessons learned