Implementation of the PISA-based Test for Schools in Mexico: Security and Confidentiality Procedures

Introduction

Knotion, as the National Service Provider (NSP) of the PISA-based Test for Schools (PBTS) in Mexico, will comply with OECD's standardized processes and recommendations concerning the implementation and distribution of the PBTS.

A main aspect of the development of PBTS operations is ensuring that all materials, methods and data are unconditionally secured and protected from potential information leaks and breaches.

This document renders Knotion's official stance on PBTS data security, prevention of information leaks, and test-takers' identity protection.

Objectives

- To stipulate the factors in the Knotion Ecosystem that will contribute towards the security and confidentiality of PISA-based Test for Schools data.
- To establish the procedures for securing and protecting PISA-based Test for Schools data.
- To establish the procedures for securing and protecting test-takers personal and sensible data.

Agents involved

Identifying every agent involved in the end-to-end process of implementing the PBTS is key for detecting potential threats to data security and privacy. For each of the agents listed below, we hypothesize about their potential *malefic* intentions, which we will address in detail under Information Leakage Prevention, Data Security and Identity Protection sections.

- *External contractors.* Since they already are approved OECD Service Providers, external contractors don't represent a major threat in information security. However, besides the contract between Knotion and the external provider, we will emphasize on appending a Non-Disclosure Agreement to protect any sensible materials and data.
- *School Coordinators.* As direct employees at each target school, school coordinators collaborate externally with Knotion and OECD, which represents a potential source of information leakage. School Coordinators will be required to sign a Non-Disclosure Agreement with Knotion.
- *Test Administrators.* Similarly to school coordinators, test administrators will be required to sign a NDA at the beginning of their collaboration with Knotion.
- *Test-takers.* Due to the expected volume of test-takers, they represent the biggest threat in terms of potential information leakages. The possible information leakage scenarios are counteracted with Mobile Device Management functionalities, this strategy is detailed under the *Information Leakage Prevention* section. The identity of test-takers will also be protected from any external party, such strategy is detailed under the *Identity Protection* section.
- *Unknown agents.* External agents, not affiliated to the OECD nor Knotion, i.e. hackers, may have interest in breaching Knotion's PBTS database. The cybersecurity strategy to counteract these potential attacks is covered in detail under the Data Security section.

Information Leakage Prevention

- All agents involved in the Knotion-PBTS operations, except for test-takers, shall sign a Non-Disclosure and Confidentiality Agreement (NDA) with Knotion. A template of such NDA is included in the *Appendix 1*.
- In order to prevent information leakage from the test-taker side, we have identify the two possible scenarios:
    a. *Implementation of PBTS in a Knotion School.* Each school in the Knotion Ecosystem is already equipped with the necessary infrastructure for daily Knotion operations. In these schools, Knotion will implement the digital PBTS. Procedures for information leakage prevention in this scenario, are detailed under *Mobile Device Management functionalities*.
    b. *Implementation of PBTS in a non-Knotion School.* As we cannot assume that a given non-Knotion school will have the necessary technology infrastructure, Knotion would either implement the paper-based PBTS or the digital PBTS, according to the school's preferences. Now, we have two possible cases:
        - *Paper-based PBTS.* Regular test-taking cautionary measures will be taking.
        - *Digital PBTS.* Procedures for information leakage prevention in this scenario are detailed under *Mobile Device Management functionalities* below.
- As an additional cautionary measure, no agent involved will have access to reproducible digital or paper test files.

Mobile Device Management functionalities

A key part of the Knotion Ecosystem is the delivery of academic content through tablets. For day to day classroom activities, Knotion's Mobile Device Management system (MDM) allows teachers to manage virtually all functionalities of students' tablets. For PBTS matters, the following functionalities can be fully and selectively managed:

a. *Screenshot prevention*. MDM can lock any given tablet's home button —either physical or assistive touch—, thus disabling the screenshot functionality. This will prevent PBTS information to be captured and shared after the test-taking timeframe.
b. *Mobile application lock*. MDM can prevent any given Knotion tablet to open any number of determined mobile applications; this functionality would ensure that only the test application is active during the timeframe determined, for instance.
c. *Connectivity lock*. MDM can prevent any given Knotion tablet to connect to any Internet or Intranet network, activate or deactivate Bluetooth and device-to-device connections. This will prevent PBTS information to be shared among test-takers and external parties.
d. *PBTS availability lock.* MDM allows to define any time-frame in which the PBTS will be available for test-takers, test administrators and school coordinators. Furthermore, this functionality allows to make the test available/unavailable at discretion of the OECD and Knotion.

Identity Protection

Since the implementation of PBTS by Knotion will be in Mexican schools, we will adhere to the Mexican law regarding personal data management for research and commercial purposes, *Ley Federal De Protección De Datos Personales En Posesión De Los Particulares* (http://www.diputados.gob.mx/LeyesBiblio/doc/LFPDPPP.doc). The Privacy Statement, crafted according to this Mexican Law, can be found in *Appendix 2*.

As PBTS collected data will be used for research purposes, and informed consent explaining the purpose of the test and nature of the data collected, needs to be signed by each test-taker parent or legal representative to ensure that they agree with their data being collected and analyzed for research purposes, including the transmission of such data to the OECD.
A template of such informed consent is included in *Appendix 3.*

Data Security

The digital version of the PBTS in Mexico will be implemented complying with high-grade cyber security standards for data encryption and transmission, such as Transport Layer Security (TLS) and Secure Socket Layer (SSL) cryptographic protocols, and industry-standard user authentication, such as OAuth 2.0 authentication scheme and bearer API tokens with 256-bits of entropy.

All PBTS data will be transferred from the PBTS application via a RESTful API using TLS/SSL protocols over a secure HTTP connection. Knotion servers use perfect forward secrecy to encrypt data using 256-bit Advanced Encryption Standards, and require that all API calls are authenticated individually, ensuring that authorized API tokens are provided each time the PBTS data is accessed.

Knotion's in-cloud data centers enable enhanced prevention of data breaches by being isolated from the public web, through a bastion server; in case of a cyber attack, the bastion host will *absorb the hits* by replicating itself as many times as needed so that the attackers keep their efforts focused on this host, while the PBTS data lies secure in the private cloud, inaccessible from these external parties.

Appendices

Appendices	Description	Link
Appendix 1	Non-Disclosure Agreement	https://goo.gl/nFzQ09
Appendix 2	Privacy Policy Statement	https://goo.gl/jQyB5t
Appendix 3	Informed Consent	https://goo.gl/OM9kZi