Privacy Impact Assessment

Maintaining security and privacy of district data

Highlights

- **Improve** management of risks, compliance and governance as it relates to data
- **Align** your use of 3rd party applications to privacy requirements
- **Generate** effective risk-mitigation strategies related to third party applications
- **Improve** confidence in data security and privacy across systems

Why Develop Privacy Impact Assessments?

Data security is top of mind in many districts, due in part, to the breaches taking place across the country and around the world. Significant efforts to protect the privacy of personal information are underway as illustrated by the General Data Protection Regulation for the European Union which comes into effect in May 2018.

Section 69(5.3) of the Freedom of Information and Protection of Privacy Act (FOIPPA) requires the head of a public body to conduct a Privacy Impact Assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. As school districts are public bodies, PIAs are required for any systems that may include personal information of staff and/or students.

All school districts are using third party applications where student and staff information is stored either on-premises, hosted at a 3rd party location or in the cloud. This data may be backed up to different locations depending on the application and the backup policy that is followed at the district level. Adding to this complexity, a disaster recovery program may cause duplicates of the data to be hosted in another location.

Understanding the Security Posture of Your Data

The goal of a Privacy Impact Assessment is to ensure confidence in the security of private data, both in storage and while it is in transit between services. As districts continue to develop their awareness of security vulnerabilities, understanding the security posture of their data, from entry to transit, storage, backup, and recovery, becomes critical.

This increasing concern in protecting personal data has also meant that the development of Privacy Impact Assessments for each 3rd party application has generally become an additional responsibility of the district IT team.

Solution Offering:

The IBM K-12 Privacy Impact Assessment Service leverages IBM Intellectual Property and industry leading practices to assist you in the creation of the PIAs required by your district.

We help by examining all pathways of your data, from entry to editing, backup and transit. We then identify the risks and mitigation strategies for each step, which are also included in the completion of your PIA document.

IBM's deep understanding of data storage and transit, as well as our extensive knowledge of applications in K-12 environments, ensures confidence in the security and privacy of your data.

Developing a Privacy Impact Assessment

IBM consultants will meet with district staff to confirm goals, understand levels of risk tolerance, review policy and procedures currently in place, determine roles and responsibilities for data security, and determine key stakeholders required to provide the necessary information to fulfill proper PIA documentation. We will also generate a template to streamline future PIA development processes.

Primary activities include:

1. Working with the vendor of the associated application to understand user creation, access rights and levels, data creation processes, data-editing processes, data storage and the format of data in storage and in-transit.
2. Creating visuals that outline the data pathways and the users responsible for the data entry, edits and management along the path.
3. Outlining associated risks related to the data and the mitigation strategies in place to meet acceptable risk tolerance.
4. Generating the final Privacy Impact Assessment documentation in a format that can be submitted for review by the Privacy Commission.

Why IBM?

IBM Canada K-12 Education includes a team of former Educational Technology Leaders that understand the flow of information while using 3rd party services. Our team members are knowledgeable and experienced in assisting districts in identifying the processes and technical requirements needed, and expanding the decision-making processes required, to maintain the security of data across systems.

IBM provides the expertise to:

1. Identify risks and mitigation strategies aligned with district levels of risk tolerance
2. Align your PIA's with provincial and Canadian leading practices
3. Improve confidence in the overall security and privacy of your data.

For more information

To learn more about IBM K-12 **Privacy Impact Assessment**, please contact your IBM Marketing Representative. For more information on all our IBM K-12 Consulting and Professional Services, visit: https://www.ibm.com/industries/education/canada-k-12-service-briefs

IBM Corporation
3600 Steeles Ave. East
Markham, ON L3R 9Z7 Canada
April 2018